Imię i nazwisko: _____ Data: _____ Wynik: _____

Oprogramowanie antywirusowe i punkty końcowe Przewodnik po ochronie

Wykrywanie sygnaturowe, heurystyka, monitorowanie zachowania, piaskownica (sandboxing), aktualizacje

PRZEGLĄD MATERIAŁU: OPROGRAMOWANIE ANTYWIRUSOWE

CHRONIONY
SZYFROWANIE DANYCH
Standard AES 256-bitowy

ZGODNY
STANDARDY GLOBALNE
Ramy prawne RODO (GDPR) i CCPA

ZERO TRUST
POLITYKA DOSTĘPU
Uwierzytelnianie wieloskładnikowe

Witaj! Ten pakiet ćwiczeń przeprowadzi cię przez oprogramowanie antywirusowe i ochronę punktów końcowych. Poznasz bazy sygnatur, skanery heurystyczne, monitorowanie zachowań, pliki wirtualne w piaskownicy i ograniczanie fałszywych alarmów.

PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj cyberbezpieczeństwo i zapobieganie zagrożeniom.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

Otwórz przewodnik VPN.com po cyberbezpieczeństwie

URL: https://www.vpn.com/pl/cyberbezpieczenstwo/antywirus/

Twoja ścieżka nauki: strategia antywirusowa

- Rozróżnij wykrywanie złośliwego oprogramowania oparte na sygnaturach i heurystyczne.
- Zrozum protokoły monitorowania zachowania i izolacji w piaskownicy.
- Oceń wpływ skanowania w czasie rzeczywistym na wydajność systemu i punktów końcowych.
- Ograniczaj fałszywie pozytywne klasyfikacje za pomocą weryfikacji certyfikatów cyfrowych.
- Zarządzaj codzienną dystrybucją aktualizacji definicji na firmowych punktach końcowych.

INSTRUKCJE: PRZEWODNIK PO PROGRAMACH ANTYWIRUSOWYCH

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu ochrony antywirusowej punktów końcowych. Zakończ zadaniem dodatkowym Myśl szybko.

OCHRONA ANTYWIRUSOWA I SKANOWANIE SYGNATUR (WPROWADZENIE)

Oprogramowanie antywirusowe chroni punkty końcowe, wykrywając, izolując w kwarantannie i usuwając złośliwe oprogramowanie. Nowoczesne systemy łączą bazy sygnatur (dopasowujące znane skróty zagrożeń) z heurystyką (analizującą strukturę pliku) i monitorowaniem zachowania, aby wykrywać exploity typu zero-day.

PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. **1. Jakie jest ograniczenie wykrywania opartego na sygnaturach?**
   - A. Nie potrafi wykryć nieznanego lub zmodyfikowanego złośliwego oprogramowania
   - B. Generuje wiele fałszywych alarmów
   - C. Wymaga dużej mocy obliczeniowej procesora
   - D. Działa tylko po połączeniu z internetem

2. **2. W jaki sposób skanery heurystyczne wykrywają nowe warianty złośliwego oprogramowania?**
   - A. Przez identyfikowanie podejrzanych wzorców i struktur kodu
   - B. Przez dopasowywanie skrótów plików do bazy zagrożeń
   - C. Przez automatyczne usuwanie wszystkich niepodpisanych plików wykonywalnych
   - D. Przez wysłanie każdego pliku do publicznego folderu w chmurze

3. **3. Jaki jest cel uruchamiania w piaskownicy (sandbox) w programie antywirusowym?**
   - A. Izolowanie i analizowanie plików w bezpiecznym wirtualnym skarbcu
   - B. Przyspieszanie transferu lokalnej kopii zapasowej systemu plików
   - C. Aktualizowanie poprawek zabezpieczeń lokalnego systemu operacyjnego
   - D. Kompresowanie dużych plików dokumentów w celu oszczędzania miejsca

4. **4. Która metoda wykrywania oznacza zagrażające zachowania w czasie rzeczywistym?**
   - A. Analiza behawioralna monitorująca działania oprogramowania
   - B. Przegląd dawnych dzienników wykonywany w nocy
   - C. Ręczne zgłaszanie przez użytkowników wolno działających aplikacji
   - D. Cotygodniowe ręczne przeglądy zainstalowanych programów

5. **5. Dlaczego regularne aktualizacje definicji są krytyczne dla skanerów?**
   - A. Aby zasilać silniki sygnatur identyfikatorami zagrożeń z bazy danych
   - B. Aby zwiększyć taktowanie procesora podczas operacji
   - C. Aby zmienić globalne czasy buforowania serwerów nazw DNS
   - D. Aby autoryzować ustawienia plików cookie przeglądarki

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie (prawda/fałsz) 6

6. Wykrywanie sygnaturowe porównuje kryptograficzne skróty plików z listami w bazie danych.

- ◯ Prawda
- ◯ Fałsz

7 Pytanie (prawda/fałsz) 7

7. Skanery heurystyczne mogą wywoływać fałszywe alarmy dla bezpiecznych plików.

- ◯ Prawda
- ◯ Fałsz

8 Pytanie (prawda/fałsz) 8

8. Sandbox pozwala złośliwemu oprogramowaniu na dostęp do plików sieciowych bez ograniczeń.

- ◯ Prawda
- ◯ Fałsz

9 Pytanie (prawda/fałsz) 9

9. Skanowanie behawioralne blokuje pliki, gdy wykazują złośliwe działania.

- ◯ Prawda
- ◯ Fałsz

10 Pytanie (prawda/fałsz) 10

10. Standardowe oprogramowanie antywirusowe całkowicie zatrzymuje wszystkie ataki zero-day.

- ◯ Prawda
- ◯ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Tradycyjny skaner identyfikuje znane malware, dopasowując je do wzorców; taki wzorzec to _____ .

2. Metoda analizowania wzorców w kodzie plików to _____ .

3. Programy antywirusowe izolują podejrzane pliki w środowisku, które nazywa się _____ .

4. Monitorowanie w czasie rzeczywistym obserwuje działania programów pod kątem podejrzanej aktywności; ten typ analizy to _____ .

5. Aby rozpoznawać nowe zagrożenia, skanery codziennie pobierają do bazy danych nowe _____ .

6. Bezpieczne programy oznaczone jako malware wywołują _____ .

BANK SŁÓW

AKTUALIZACJE	ANALIZA ZACHOWAŃ	FAŁSZYWY ALARM	HEURYSTYKA
PIASKOWNICA	ROBAK KOMPUTEROWY	SYGNATURA	ZAPORA SIECIOWA

Wpisz tutaj swoje odpowiedzi:

1.
2.
3.
4.
5.
6.

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

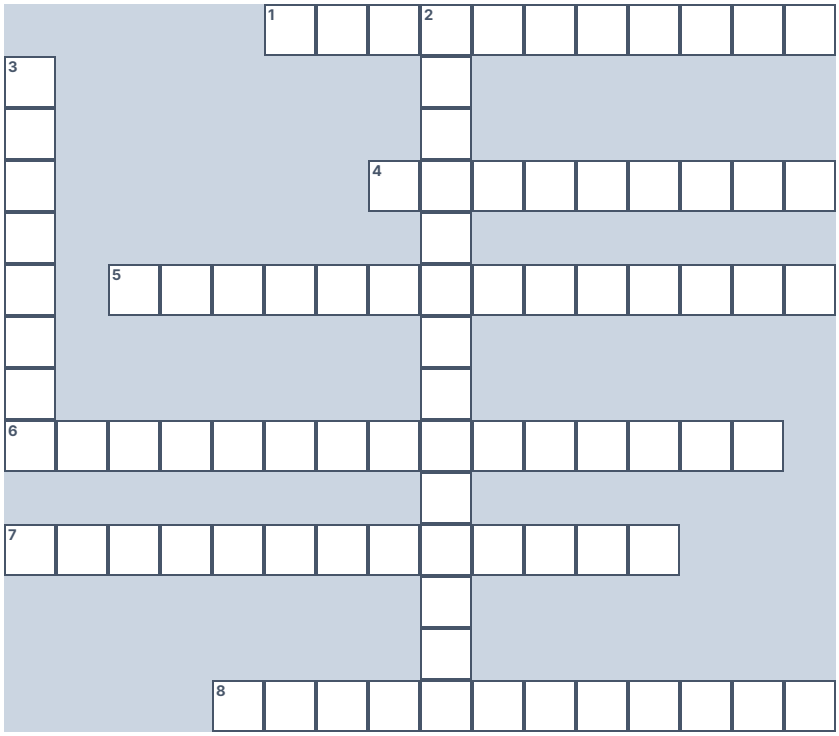
DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

☐	1. Sygnatura skrótu	A	Izolowanie podejrzanych plików, aby zapobiec narażeniu lokalnego systemu.
☐	2. Heurystyka kodu	B	Pakiet oprogramowania skanujący i chroniący punkty końcowe przed exploitami.
☐	3. Piaskownica plików	C	Monitorowanie działań uruchomionego oprogramowania pod kątem wzorców złośliwego działania.
☐	4. Skanowanie zachowania	D	Unikalny kryptograficzny odcisk w bazie danych służący do identyfikowania znanych zagrożeń.
☐	5. Codzienne aktualizacje	E	Bezpieczne wirtualne środowisko testowe, w którym można bezpiecznie uruchamiać niezaufany kod.
☐	6. Fałszywy alarm	F	Regularne pobieranie definicji zasilających bazę zagrożeń.
☐	7. Izolacja zagrożeń	G	Analiza oparta na regułach oznaczająca pliki z podejrzanym układem kodu.
☐	8. Program antywirusowy	H	Alert bezpieczeństwa błędnie klasyfikujący bezpieczne oprogramowanie jako złośliwe.

Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.



POZIOMO

1. Bezpieczne wirtualne środowisko testowe, w którym można bezpiecznie uruchamiać niezaufany kod (11)

4. Pakiet oprogramowania skanujący i chroniący urządzenia końcowe przed exploitami (9)

5. Analiza oparta na regułach, oznaczająca pliki o podejrzanej budowie kodu (14)

6. Monitorowanie działań uruchomionego oprogramowania pod kątem wzorców złośliwego działania (15)

7. Alert bezpieczeństwa błędnie klasyfikujący bezpieczne oprogramowanie jako malware (13)

8. Regularne pobieranie definicji zasilających bazę zagrożeń (12)

PIONOWO

2. Unikalny kryptograficzny odcisk w bazie danych służący do identyfikacji znanych zagrożeń (14)

3. Zamknięcie podejrzanych plików, aby zapobiec narażeniu lokalnego systemu (8)

Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej. HASŁA POZIOME HASŁA PIONOWE

POZIOMO

1 poziomo: Bezpieczne wirtualne środowisko testowe, w którym można bezpiecznie uruchamiać niezaufany kod (11 liter):

4 poziomo: Pakiet oprogramowania skanujący i chroniący urządzenia końcowe przed exploitami (9 liter):

5 poziomo: Analiza oparta na regułach, oznaczająca pliki o podejrzanej budowie kodu (14 liter):

6 poziomo: Monitorowanie działań uruchomionego oprogramowania pod kątem wzorców złośliwego działania (15 liter):

7 poziomo: Alert bezpieczeństwa błędnie klasyfikujący bezpieczne oprogramowanie jako malware (13 liter):

8 poziomo: Regularne pobieranie definicji zasilających bazę zagrożeń (12 liter):

PIONOWO

2 pionowo: Unikalny kryptograficzny odcisk w bazie danych służący do identyfikacji znanych zagrożeń (14 liter):

3 pionowo: Zamknięcie podejrzanych plików, aby zapobiec narażeniu lokalnego systemu (8 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

A Ę O K Ń A Ć A N C Ć G I Ą Ą
Ó R Ł P W J T N I Ź S Ę U Ź S
M G Y X E C H A Ę R Y T D Ń U
R K R Ć J A T L S Ł G P O Ł N
A Ś P H C L L I P H N Ź K Ó Ł
L X I V A O Ń Z Z Q A Q A Ą A
A A A Ł Z Z Ó A N Ą T Ł K I N
Y Ę S J I I Ń Z Z B U Ż Y Ż T
W Ź K B L N V A Y M R C T Ę Y
Y Ó O X A P Q C Y G A D S Ź W
Z B W X U Ł E H G G H Ż Y X I
S C N O T Q K O Y Y A R R L R
Ł Ż I A K N R W Ż R S M U F U
A Ś C W A F Ł A X J H B E Ź S
F C A B Ź O V Ń Ż O A Ż H U T

LISTA SŁÓW

SYGNATURAHASHA HEURYSTYKAKODU PIASKOWNICA ANALIZAZACHOWAŃ
AKTUALIZACJE FAŁSZYWYALARM IZOLACJA ANTYWIRUS

Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

TERMINY ZE SŁOWNICZKA

- **A. SYGNATURAHASHA**
- **B. HEURYSTYKAKODU**
- **C. PIASKOWNICA**
- **D. ANALIZAZACHOWAŃ**
- **E. AKTUALIZACJE**
- **F. FAŁSZYWYALARM**
- **G. IZOLACJA**
- **H. ANTYWIRUS**

DEFINICJE I POLA DOPASOWANIA

1. Monitorowanie działań uruchomionego oprogramowania pod kątem wzorców złośliwego działania.
2. Pakiet oprogramowania skanujący i chroniący urządzenia końcowe przed exploitami.
3. Regularne pobieranie definicji zasilających bazę zagrożeń.
4. Analiza oparta na regułach, oznaczająca pliki o podejrzanej budowie kodu.
5. Zamknięcie podejrzanych plików, aby zapobiec narażeniu lokalnego systemu.
6. Unikalny kryptograficzny odcisk w bazie danych służący do identyfikacji znanych zagrożeń.
7. Bezpieczne wirtualne środowisko testowe, w którym można bezpiecznie uruchamiać niezaufany kod.
8. Alert bezpieczeństwa błędnie klasyfikujący bezpieczne oprogramowanie jako malware.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z cyberbezpieczeństwem. Wpisz odpowiedzi w przygotowanych polach.

1. ATRHUGYASS HAAN
2. KAIPCOAINW S
3. AKZIJATLEAC U
4. LJACAIZO
5. AUOEYKYUSK THDR
6. OAWAZZCAŃ HANALI
7. LAYYFAAZMR ŁWS
8. SWUAYNIRT

Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

1	Powody, dla których warto aktualizować oprogramowanie			
2	Osoby, które możesz poprosić o pomoc IT			
3	Rzeczy do zrobienia, gdy antywirus coś znajdzie			
4	Oznaki wirusa komputerowego			
5	Rzeczy, które trafiają do kwarantanny			
6	Miejsca, w których ukrywają się wirusy			
7	Informacje, których nigdy nie powinieneś udostępniać			
8	Rodzaje złośliwego oprogramowania			
9	Narzędzia bezpieczeństwa, które znasz			
10	Rzeczy, które skanuje antywirus			
11	Rzeczy, z których robisz kopie zapasowe			
12	Urządzenia, które można zhakować			
13	Programy antywirusowe, które znasz			
14	Powody fałszywych alarmów			
15	Bezpieczne nawyki, które możesz zacząć już dziś			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

STUDIUM PRZYPADKU 1: SKANOWANIE SYGNATUROWE A HEURYSTYCZNE



Scenariusz: Pracownik pobiera narzędzie niestandardowe, zbudowane wewnętrznie przez inny zespół. Skaner sygnaturowy je przepuszcza, ale skaner heurystyczny oznacza je jako podejrzane.

Pytanie do dyskusji: Wyjaśnij, dlaczego tak się stało i jak sprawdzić, czy plik jest bezpieczny.

STUDIUM PRZYPADKU 2: OBSŁUGA FAŁSZYWYCH ALARMÓW



Scenariusz: Programista kompiluje swoją aplikację. Systemowy antywirus oznacza nowy plik wykonywalny jako złośliwe oprogramowanie i poddaje go kwarantannie.

Pytanie do dyskusji: Opisz ryzyka związane z dodawaniem do białej listy i wskaż prawidłową ścieżkę rozwiązania.

Punkt kontrolny 9: Odszyfruj szyfr

Specjalista ds. cyberbezpieczeństwa chroni zasoby sieciowe przed cyberprzestępcami. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

KLUCZ SZYFROWANIA LITERA-LICZBA

A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12
J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24
S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35

30	32	14	24	32	13		18	20	30	7		17	1	15	30	1	24	7
1	18	1	15	12	33	2		11	7	28	24	32	25	27	32	4	33	18	2

14	20	6	28

Odszyfrowana wiadomość:

WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część A)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q1: Jak oprogramowanie antywirusowe identyfikuje złośliwe oprogramowanie?

Identyfikuje złośliwe oprogramowanie za pomocą dopasowywania sygnatur z bazy danych, heurystycznej analizy układu kodu i monitorowania zachowania w czasie rzeczywistym.

Q2: Czym jest wykrywanie oparte na sygnaturach?

To metoda skanowania, która dopasowuje kryptograficzne skróty plików do list z bazy znanych zagrożeń złośliwego oprogramowania.

Q3: Czym jest skaner heurystyczny?

Heurystyka analizuje strukturę pliku i instrukcje kodu, oznaczając podejrzane wzorce typowe dla wariantów złośliwego oprogramowania.

Q4: Co oznacza, że plik został poddany kwarantannie?

Antywirus przenosi plik do bezpiecznego, odizolowanego folderu i blokuje jego uruchomienie, aby chronić system operacyjny.

Q5: Czym jest fałszywy alarm antywirusa (false positive)?

To błąd, w którym legalne, bezpieczne oprogramowanie jest nieprawidłowo oznaczane przez algorytmy skanowania jako złośliwe.

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część B)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Jak monitorowanie zachowania chroni systemy?

Monitoruje działające oprogramowanie w czasie rzeczywistym, blokując procesy próbujące wprowadzić podejrzane zmiany, takie jak wstrzykiwanie kodu.

Q7: Dlaczego testowanie w piaskownicy jest ważne?

Piaskownica uruchamia niezaufane pliki w izolowanej maszynie wirtualnej, bezpiecznie obserwując ich działania bez narażania systemu.

Q8: Jak często powinny aktualizować się definicje antywirusowe?

Skanery powinny aktualizować definicje codziennie lub co godzinę, aby rozpoznawać nowo odkryte odmiany złośliwego oprogramowania.

Q9: Jaka jest różnica między antywirusem a EDR?

Program antywirusowy skupia się na skanowaniu plików, natomiast Endpoint Detection and Response (EDR) zapewnia śledzenie zagrożeń w całej sieci i ich izolowanie.

Q10: Czy mogę uruchomić dwa programy antywirusowe jednocześnie?

Nie. Uruchomienie dwóch aktywnych skanerów powoduje konflikty w systemie, spowalnia wydajność i może blokować nawzajem ich działanie.

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część C)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q1: Jak reguły heurystyczne ograniczają omijanie zabezpieczeń przez zagrożenia?

Heurystyka analizuje ogólne wzorce zagrożeń zamiast konkretnych sygnatur, wychwytując zmodyfikowane warianty znanych rodzin złośliwego oprogramowania.

Q2: Czym jest wirus polimorficzny?

To złośliwe oprogramowanie, które przy każdym uruchomieniu zmienia układ pliku i procedurę deszyfrowania, przez co skanowanie sygnatur jest nieskuteczne.

Q3: Jak piaskownice wykrywają unikanie wykrycia przez maszyny wirtualne?

Nowoczesne piaskownice symulują kliknięcia myszą i czas działania systemu, oszukując złośliwe oprogramowanie zaprojektowane tak, aby ukrywać się podczas działania w maszynach wirtualnych.

Q4: Jakie są formaty pobierania aktualizacji sygnatur?

Aktualizacje to zazwyczaj lekkie, przyrostowe pliki różnicowe binarne, które minimalizują zużycie przepustowości sieci klienta.

Q5: Jak agenci punktów końcowych zarządzają lokalnymi skanowaniami?

Agenci wykonują lekkie kontrole w tle, przekazując głębokie wyszukiwania skrótów kryptograficznych do chmurowych baz danych zagrożeń.

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część D)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q6: Czym jest skanowanie w poszukiwaniu rootkitów?

Skanuje tablice pamięci na poziomie jądra, omijając interfejsy API systemu operacyjnego, które rootkity przechwytują, aby ukryć swoje aktywne wątki.

Q7: Jak skanowanie zachowania blokuje ransomware?

Wykrywa zautomatyzowane pętle masowego szyfrowania plików i kończy proces hosta, zanim bazy danych systemu zostaną zablokowane.

Q8: Czym jest weryfikacja certyfikatu podpisywania kodu?

Skanery sprawdzają cyfrowe podpisy kodu względem zaufanych głównych urzędów certyfikacji, weryfikując tożsamość twórcy oprogramowania.

Q9: Jak packery wpływają na silniki skanujące?

Packery kompresują lub szyfrują ładunki złośliwego oprogramowania. Skanery muszą rozpakować plik w pamięci, zanim zostaną uruchomione dopasowania sygnatur.

Q10: Jak narzędzia EDR automatyzują izolację?

Agenty EDR poddają kwarantannie zainfekowane punkty końcowe na poziomie sieci, blokując ruch boczny, a jednocześnie zachowując dostęp dla analityków.

Część 11: 10 faktów o cyberbezpieczeństwie z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące naruszeń bezpieczeństwa, mechanizmów obronnych i standardów zgodności.

1. WGLĄD W BEZPIECZEŃSTWO

Bazy sygnatur przechowują skróty znanego złośliwego oprogramowania, więc zupełnie nowe lub zmienione pliki są pomijane do czasu aktualizacji definicji.

2. WGLĄD W BEZPIECZEŃSTWO

Silniki heurystyczne mogą oznaczyć niektóre nowe warianty złośliwego oprogramowania, zanim powstaną sygnatury, kosztem większej liczby fałszywych alarmów.

3. WGLĄD W BEZPIECZEŃSTWO

Fałszywie pozytywne alerty kosztują zespoły IT czas poświęcony na weryfikację i przywracanie plików, które błędnie poddano kwarantannie.

4. WGLĄD W BEZPIECZEŃSTWO

Złośliwe oprogramowanie polimorficzne zmienia swój kod z każdą kopią, więc obrońcy łączą sygnatury z kontrolami heurystycznymi i behawioralnymi.

6. WGLĄD W BEZPIECZEŃSTWO

Autorzy złośliwego oprogramowania piszą niestandardowy kod sprawdzający środowiska piaskownicy i opóźniający wykonanie, aby ominąć liczniki czasu.

5. WGLĄD W BEZPIECZEŃSTWO

Chmurowe silniki antywirusowe porównują skróty podejrzanych plików z dużymi internetowymi bazami zagrożeń niemal w czasie rzeczywistym.

7. WGLĄD W BEZPIECZEŃSTWO

Dostawcy regularnie wysyłają na urządzenia końcowe aktualizacje definicji, aby skanery mogły rozpoznawać nowo potwierdzone zagrożenia.

8. WGLĄD W BEZPIECZEŃSTWO

Monitory behawioralne ransomware są nastawione na określone wywołania API Win32 związane z szyfrowaniem plików i usuwaniem kopii w tle.

9. WGLĄD W BEZPIECZEŃSTWO

Prawidłowe podpisy kodu mogą zmniejszyć ryzyko fałszywych alarmów, ale podpisane pliki są nadal skanowane, ponieważ złośliwe oprogramowanie również może być podpisane.

10. WGLĄD W BEZPIECZEŃSTWO

Rootkity modyfikują struktury jądra systemu, co wymaga specjalistycznych skanerów uruchamianych przy starcie systemu, aby je wykryć i usunąć.

Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów NIST, OWASP i zgodności z przepisami o ochronie prywatności danych. PUBLIKACJE NAUKOWE I BRANŻOWE

PUBLIKACJE NAUKOWE I BRANŻOWE

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.

https://csrc.nist.gov/pubs/sp/800/61/r3/final

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1 SYGNATURY **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Skanowanie sygnaturowe opiera się na znanych skrótach z bazy danych, przez co nie wykrywa nieznanego ani zmodyfikowanego złośliwego oprogramowania. Źródło: OWASP Secure Configuration.

2 Pytanie 2 HEURYSTYKA **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Heurystyka analizuje układ kodu i polecenia, aby identyfikować podejrzane cechy nowych wariantów zagrożeń. Źródło: Center for Internet Security (CIS).

3 Pytanie 3 URUCHAMIANIE W PIASKOWNICY **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Piaskownica uruchamia podejrzane pliki w izolowanej maszynie wirtualnej, aby bezpiecznie obserwować zachowanie podczas wykonywania. Źródło: NIST Digital Identity.

4 Pytanie 4 BEHAWIORALNY **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Skanowanie behawioralne monitoruje uruchomione programy w czasie rzeczywistym, aby blokować nieautoryzowane zmiany w systemie. Źródło: Center for Internet Security (CIS).

5 Pytanie 5 AKTUALIZACJE **Poprawna odpowiedź: A**

UWAGA DLA NAUCZYCIELA

Skanery pobierają codzienne przyrostowe aktualizacje definicji, aby pozostać zsynchronizowane z krajobrazem zagrożeń. Źródło: OWASP Secure Configuration.

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Pytanie 6** SYGNATURY **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Narzędzia sygnaturowe obliczają skróty kryptograficzne i porównują je z bazą danych skrótów znanych zagrożeń. Źródło: OWASP Secure Configuration.

7 **Pytanie 7** HEURYSTYKA **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Silniki heurystyczne stosują układy oparte na regułach, które mogą oznaczać legalne, bezpieczne pliki jako podejrzane. Źródło: Center for Internet Security (CIS).

8 **Pytanie 8** URUCHAMIANIE W PIASKOWNICY **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Piaskownica uruchamia kod w wirtualnym kontenerze, ściśle blokując dostęp do udziałów sieciowych. Źródło: NIST Digital Identity.

9 **Pytanie 9** BEHAWIORALNY **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Monitorowanie w czasie rzeczywistym oznacza uruchomione procesy, które próbują wykonać niedozwolone zapisy lub blokowanie plików. Źródło: Center for Internet Security (CIS).

10 **Pytanie 10** **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Żaden program antywirusowy nie zatrzymuje każdego ataku zero-day; nieznane zagrożenia mogą omijać sygnatury i heurystykę.

Klucze słownictwa i kryteria oceny

Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).

PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

D 1. Sygnatura skrótu	G 2. Heurystyka kodu	E 3. Piaskownica plików	C 4. Skanowanie zachowania
F 5. Codzienne aktualizacje	H 6. Fałszywy alarm	A 7. Izolacja zagrożeń	B 8. Program antywirusowy

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 SYGNATURA	2 HEURYSTYKA	3 PIASKOWNICA	4 ANALIZA ZACHOWAŃ
5 AKTUALIZACJE	6 FAŁSZYWY ALARM		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 D – ANALIZAZACHOWAŃ	2 H – ANTYWIRUS	3 E – AKTUALIZACJE	4 B – HEURYSTYKAKODU
5 G – IZOLACJA	6 A – SYGNATURAHASHA	7 C – PIASKOWNICA	8 F – FAŁSZYWYALARM

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

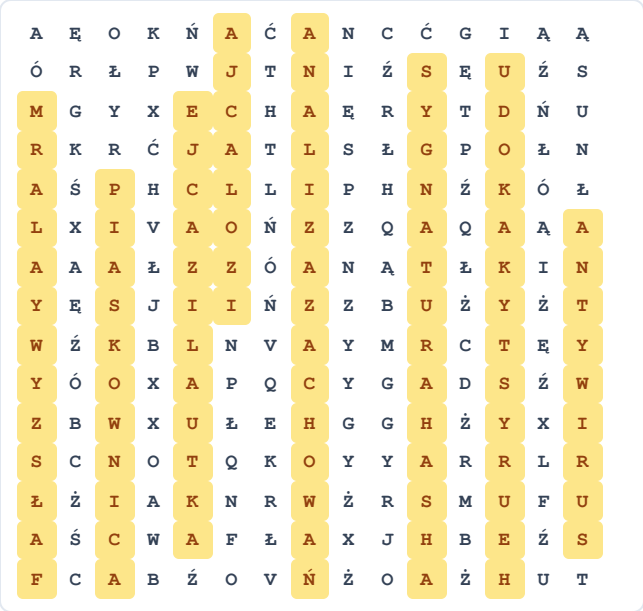
Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia Sygnatura skrótu, Heurystyka kodu i Piaskownica plików oraz podać przykład każdego z nich.

Studia przypadków:
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

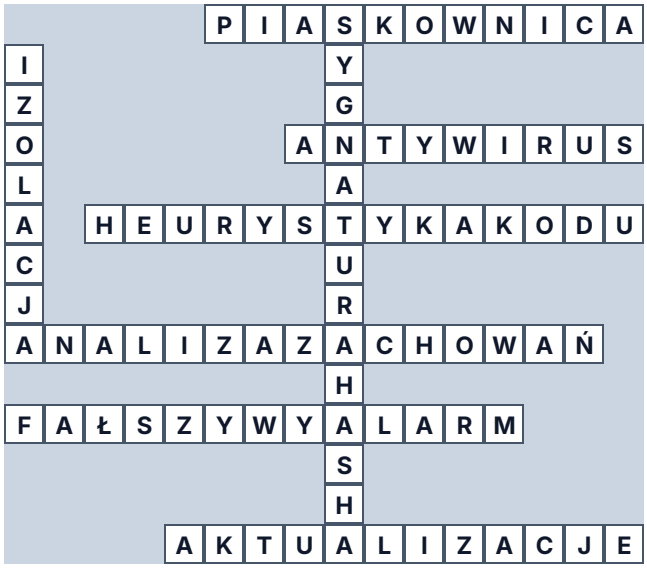
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ



ROZWIĄZANIE KRZYŻÓWKI



POZIOMO

1 poziomo: PIASKOWNICA Bezpieczne wirtualne środowisko testowe, w którym można bezpiecznie uruchamiać niezaufany kod (11 liter)

4 poziomo: ANTYWIRUS Pakiet oprogramowania skanujący i chroniący urządzenia końcowe przed exploitami (9 liter)

5 poziomo: HEURYSTYKAKODU Analiza oparta na regułach, oznaczająca pliki o podejrzanej budowie kodu (14 liter)

6 poziomo: ANALIZAZACHOWAŃ Monitorowanie działań uruchomionego oprogramowania pod kątem wzorców złośliwego działania (15 liter)

7 poziomo: FAŁSZYWYALARM Alert bezpieczeństwa błędnie klasyfikujący bezpieczne oprogramowanie jako malware (13 liter)

8 poziomo: AKTUALIZACJE Regularne pobieranie definicji zasilających bazę zagrożeń (12 liter)

PIONOWO

2 pionowo: SYGNATURAHASHA Unikalny kryptograficzny odcisk w bazie danych służący do identyfikacji znanych zagrożeń (14 liter)

3 pionowo: IZOLACJA Zamknięcie podejrzanych plików, aby zapobiec narażeniu lokalnego systemu (8 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. ATRHUGYASSHAAN — **SYGNATURAHASHA**
2. KAIPCOAINWS — **PIASKOWNICA**
3. AKZIJATLEACU — **AKTUALIZACJE**
4. LJACAIZO — **IZOLACJA**
5. AUOEYKYUSKTHDR — **HEURYSTYKAKODU**
6. OAWAZZCAŃHANALI — **ANALIZAZACHOWAŃ**
7. LAYYFAAZMRŁWS — **FAŁSZYWYALARM**
8. SWUAYNIRT — **ANTYWIRUS**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"WYKRYJ NOWE MALWARE ANALIZĄ HEURYSTYCZNĄ KODU"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Skanowanie sygnaturowe a heurystyczne

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Pracownik pobiera niestandardowe narzędzie stworzone wewnętrznie przez inny zespół. Skaner sygnaturowy je przepuszcza, ale skaner heurystyczny oznacza je jako podejrzane.
- Zalecana strategia i rozwiązanie: Dlaczego do tego doszło: Skanowanie sygnaturowe sprawdza skróty plików; ponieważ plik jest autorski, nie ma go w bazie zagrożeń. Heurystyka analizuje strukturę i oznaczyła podejrzane działania (np. zapisy do rejestru). Weryfikacja: Uruchom plik w piaskownicy (sandbox), aby obserwować jego działania, sprawdź podpisy cyfrowe i prześlij skrót do portali z danymi o zagrożeniach.

B Studium przypadku 2: Obsługa fałszywych alarmów

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Programista kompiluje swoją aplikację. Systemowy antywirus oznacza nowy plik wykonywalny jako złośliwe oprogramowanie i przenosi go do kwarantanny.
- Zalecana strategia i rozwiązanie: Ryzyka białej listy: Pomijanie skanerów może pozwolić na uruchomienie prawdziwego, zainfekowanego kodu. Ścieżka rozwiązania: Prześlij plik do producenta antywirusa do analizy, podpisz kod cyfrowo za pomocą urzędów certyfikacji i tymczasowo skonfiguruj wyjątki dla określonych folderów zamiast wyłączać antywirusa.