

OPROGRAMOWANIE ANTYWIRUSOWE PRZEZNACZONE DLA JEDNOSTKI EDUKACYJNEJ

100 LICENCJI / 36 MIESIĘCY

PROGRAM MUSI
WSPIERAĆ
NASTĘPUJĄCE
PLATFORMY:

- Microsoft Windows 10 Pro
- Microsoft Windows 11 Pro

Okres obowiązywania licencji: 36 miesięcy od 01.01.2025r.

ADMINISTRACJA
ZDALNA
W CHMURZE

- Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
- Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
- Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
- Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
- Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
- Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
- Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
- Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo,

comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

OCHRONA STACJI ROBOCZYCH

- Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- Rozwiązanie musi wspierać architekturę ARM64.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
- Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
- Rozwiązanie musi integrować się z Intel Threat Detection Technology.
- Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
- Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

- Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwić użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
 - Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

- Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
- Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
- Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).
- Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
 - Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
 - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
- Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
 - Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
 - Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
 - Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
 - Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
 - Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
 - W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

OCHRONA SERWERA

- Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
- Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
- Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

- Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

- Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
- Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
- Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
- Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
- Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
- Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
- Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

- Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

- Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonoego mikro-serwisu.

SZYFROWANIE

- System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
- System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
- Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
- Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

OCHRONA URZĄDZEŃ MOBILNYCH OPARTYCH O SYSTEM ANDROID

- Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
- Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
- Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
- Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia,
 - przywrócenie urządzenie do ustawień fabrycznych,
 - zablokowania urządzenia,
 - uruchomienie sygnału dźwiękowego,
 - lokalizację GPS.
- Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
- Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - nazwę aplikacji,
 - nazwę pakietu,
 - kategorię sklepu Google Play,
 - uprawnienia aplikacji,
 - pochodzenie aplikacji z nieznanego źródła.

OCHRONA
SERWERA
POCZTOWEGO MS
EXCHANGE

- Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
- Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
- Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
- Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
- Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
- Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
- Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
- System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
- Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystała aplikacja.
- Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
- Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

SANDBOX
W CHMURZE

- Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- Rozwiązanie musi wykorzystywać do działania chmurę producenta.
- Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
- Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
- Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
- Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.

- Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
- Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu.
- Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.

Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, Podejrzany, Szkodliwy.

- W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
- W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
- Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

OCHRONA USŁUGI MICROSOFT 365

- Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
- Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365.
- Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
- Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
- Rozwiązanie musi być dostępny w języku polskim.
- Konsola rozwiązania musi posiadać możliwość raportowania co najmniej: użytkowników, otrzymujących najwięcej spamu, użytkowników, otrzymujących najwięcej wiadomości typu „phishing”, użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, kont użytkowników, które mogą być podejrzane.
- Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
- Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej: jaka ilość wiadomości została

przeskanowania, wynik skanowania poszczególnej wiadomości, czynność podjęta przez rozwiązanie.

- Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte, na jakim koncie zostały wykryte, jakie zagrożenie zostało wykryte, podjętą czynność.
- Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
- Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
- Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
- Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej: wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, prowadzenia białych i czarnych list adresów ochrony Exchange'a Online, dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
- Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
- Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
- Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
- Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
- Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

MODUŁ
ZARZĄDZANIA
PODATNOŚCIAMI I
AKTUALIZACJAMI)

- Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
- Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
- Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.
- Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.

- Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
 - nazwę aplikacji lub systemu operacyjnego
 - punktacje CVSS
 - opis wykrytej podatności
 - wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
- Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
- Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
- Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
- Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
- Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
- Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
- Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
- Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
- Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.