



Zablokowane zagrożenie sieciowe

Do takiej sytuacji może dojść, gdy aplikacja na komputerze próbuje przestać złośliwy ruch do innego urządzenia w sieci, wykorzystując lukę w zabezpieczeniach lub nawet po wykryciu próby skanowania portu w systemie.

Typ zagrożenia i powiązany adres IP urządzenia można znaleźć w powiadomieniu. Kliknij opcję **Zmień obsługę tego zagrożenia**, aby wyświetlić następujące opcje:


Blokuj dalej — powoduje zablokowanie wykrytego zagrożenia. Jeśli chcesz wyłączyć otrzymywanie powiadomień o tego typu zagrożeniach z określonego adresu zdalnego, wybierz przycisk opcji obok opcji **Nie powiadamiaj** przed kliknięciem przycisku **Kontynuuj blokowanie**. Spowoduje to utworzenie reguły [Usługa wykrywania włamań \(IDS\)](#) o następującej konfiguracji: **Blokuj** — domyślnie, **Powiadamiaj** — nie, **Zapisuj w dzienniku** — nie.

Zezwalaj — tworzy regułę [Usługa wykrywania włamań \(IDS, Intrusion Detection Service\)](#), aby zezwolić na wykryte zagrożenie. Przed kliknięciem przycisku **Zezwalaj** wybierz jedną z następujących opcji, aby określić ustawienia reguły:

- **Powiadamiaj tylko, gdy to zagrożenie zostanie zablokowane** — konfiguracja reguły: **Blokuj** — nie, **Powiadamiaj** — nie, **Zapisuj w dzienniku** — nie.
- **Powiadamiaj zawsze, gdy ma miejsce to zagrożenie** — konfiguracja reguły: **Blokuj** — nie, **Powiadamiaj** — domyślnie, **Zapisuj w dzienniku** — domyślnie.
- **Nie powiadamiaj** — konfiguracja reguły: **Blokuj** — nie, **Powiadamiaj** — nie, **Zapisuj w dzienniku** — nie.

i Informacje widoczne w tym oknie powiadomienia mogą się różnić w zależności od rodzaju wykrytego zagrożenia.

Więcej informacji na temat zagrożeń i innych związanych z nimi terminów można znaleźć w artykułach [Typy ataków zdalnych](#) oraz [Typy wykrytych zagrożeń](#).

Aby rozwiązać problem ze zdarzeniem **Duplikaty adresów IP w sieci**, zapoznaj się z [artykułem bazy wiedzy firmy ESET](#) .

© 1992-2024 ESET, spol. s r.o. – Wszelkie prawa zastrzeżone.