# Alerty, incydenty i EDR: co robimy, gdy Defender coś znajdzie

**Poziom: średnio**

**Dotyczy: Microsoft Defender for Business, portal security.microsoft.com, Windows 11**

**Czas: ~40 min**

*Gdy Defender wykryje zagrożenie, część spraw załatwia sam, a część zgłasza dyżurnemu. Ta strona pokazuje kolejkę incydentów, automatyczną naprawę, izolację urządzenia, kwarantannę i powiadomienia e-mail, zaznaczając, co z funkcji EDR jest dostępne w Defender for Business, a czego tam nie ma. Zawiera też procedurę dyżurnego Zielonej i przykład z laptopem Kasi.*

**Skróty użyte na tej stronie (3)**

| Skrót | Co znaczy |
|---|---|
| **EDR** | Endpoint Detection and Response: ochrona stacji, która obserwuje zachowanie programów, nie tylko sygnatury |
| **IP** | Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection) |
| **VPN** | Virtual Private Network: szyfrowany tunel do sieci firmowej |

# Fiszka

Komendy PowerShell wykonujemy na urządzeniu w oknie administratora.

> Nazwy menu w portalach Microsoftu bywają zmieniane, a opisy poniżej odpowiadają stanowi z października 2026. Od 1 września 2026 roku Microsoft zmienił automatyczne dochodzenie: działa w ramach antywirusa i nie ma już przycisku ręcznego uruchomienia. Stare instrukcje z „Initiate Automated Investigation" są nieaktualne.

TYLKO ODCZYT

## Otwarcie kolejki incydentów

```
security.microsoft.com → Incidents & alerts → Incidents
```

Po wybraniu incydentu otwiera się panel boczny z tytułem alertu, listą zasobów (urządzenia, konta) i dostępnymi akcjami. Układ zakładek w pełnym widoku incydentu może się różnić w Business od Defender for Endpoint, więc opisujemy tylko to, co widzimy w panelu.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Incidents & alerts → Incidents z filtrem Severity ustawionym na High i Medium, widoczny incydent z laptopa Kasi, kolumny: nazwa, waga, status, urządzenia.

KLIKAMY W INTERFEJSIE

## Otwarcie listy zagrożonych urządzeń

```
security.microsoft.com → Home → karta Devices at risk → View details
→ wybieramy urządzenie → panel boczny z alertami i akcjami
```

TYLKO ODCZYT

## Otwarcie Action center

```
security.microsoft.com → Actions & submissions → Action center
→ zakładka Pending: akcje czekające na zatwierdzenie
→ zakładka History: akcje wykonane
```

Tu widać wszystko, co system zrobił sam (kwarantanna pliku, zatrzymanie procesu), i to, co czeka na decyzję. Bezpośredni adres: `https://security.microsoft.com/action-center`.

KLIKAMY W INTERFEJSIE

## Izolacja urządzenia od sieci

```
security.microsoft.com → Assets → Devices → wybieramy urządzenie
→ menu akcji (trzy kropki) → Isolate device → komentarz → Confirm
```

Urządzenie traci łączność z siecią, ale zachowuje połączenie z usługą Defender. Zwolnienie: ta sama ścieżka, przycisk Release from isolation. Wariant selektywny (z zachowaniem Outlooka i Teams) dokumentacja Defender for Endpoint opisuje dla Windows i macOS. Czy jest dostępny w Business, sprawdzamy w portalu na stronie urządzenia.

**□□ KLIKAMY W INTERFEJSIE**

## Uruchomienie skanu antywirusowego z portalu

```
Assets → Devices → wybieramy urządzenie → menu akcji → Run antivirus scan
→ Quick scan albo Full scan → komentarz → Confirm
```

Po wycofaniu ręcznego uruchamiania dochodzenia to jest podstawowy sposób ręcznego sprawdzenia urządzenia.

**□□ KLIKAMY W INTERFEJSIE**

## Dodanie wskaźnika blokowania pliku albo adresu

```
security.microsoft.com → Settings → Endpoints → Rules → Indicators
→ + Add item → typ: File hash, IP address, URL/Domain → akcja: Block execution albo
Allow
```

Wskaźniki (indicators) pozwalają zablokować albo dopuścić konkretny plik, adres IP lub domenę dla całej firmy. Muszą być włączone przełączniki Allow or block file i Custom network indicators (domyślnie włączone).

□□ **IP** = Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)

**□□ TYLKO ODCZYT**

## Odczyt wykrytych zagrożeń na urządzeniu: Get-MpThreatDetection

```
Get-MpThreatDetection | Select-Object InitialDetectionTime, ProcessName, Resources,
ActionSuccess
```

Pokazuje historię wykryć lokalnie, także wtedy, gdy portal jeszcze ich nie pokazuje. Pełny skan z wiersza poleceń opisuje strona Wdrożenie ochrony na stacje Windows: GPO, Intune albo RMM (`MpCmdRun.exe -Scan -ScanType 2`).

**GPO** = Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery · **RMM** = Remote Monitoring and Management: platforma do zdalnego zarządzania i monitorowania stacji roboczych

**TYLKO ODCZYT**

## Zebranie logów diagnostycznych antywirusa: MpCmdRun.exe -GetFiles

```
& "$env:ProgramFiles\Windows Defender\MpCmdRun.exe" -GetFiles
```

Wynik trafia do pliku `C:\ProgramData\Microsoft\Windows Defender\Support\MpSupportFiles.cab`. W nowszych wersjach platformy program leży w `%ProgramData%\Microsoft\Windows Defender\Platform\<wersja>`, więc gdy ścieżka nie istnieje, szukamy tam najnowszego katalogu.

**KLIKAMY W INTERFEJSIE**

## Pobranie pakietu dochodzenia: dostępność

```
Assets → Devices → wybieramy urządzenie → menu akcji → Collect investigation package
```

Dokumentacja Defender for Endpoint przypisuje tę akcję do Planu 2, a dla Business wymienia tylko skan, izolację i wskaźniki. Gdy pozycji nie ma w menu naszego urządzenia, zamiast pakietu zbieramy logi poleceniem `MpCmdRun.exe -GetFiles` z poprzedniej fiszki oraz eksport dziennika zdarzeń: `wevtutil epl Security PlikWynikowy.evtx`.

**TYLKO ODCZYT**

## Odczytanie zakodowanego polecenia PowerShell

```
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String("TekstBase64"))
```

> (gdzie `TekstBase64` to ciąg znaków po przełączniku `-EncodedCommand` albo `-enc` z wiersza poleceń z alertu)

Zakodowane polecenie PowerShell to zwykły tekst zapisany w base64 w kodowaniu UTF-16. Polecenia tylko odczytujemy, nigdy nie uruchamiamy, więc nie wklejamy go do `Invoke-Expression`. Wynik oglądamy w edytorze tekstu.

**KLIKAMY W INTERFEJSIE**

### Ustawienie powiadomień e-mail o alertach

```
security.microsoft.com → Settings → Endpoints → General → Email notifications
→ zakładka Alerts → + Create rule → nazwa, poziom ważności, odbiorcy
→ zakładka Vulnerabilities → + Create rule (opcjonalnie)
```

Odbiorcami reguł są konkretne osoby, nie grupy. Reguły nie dają się zawężać do grup urządzeń i nie działają przez role.

**TYLKO ODCZYT**

### Przydzielenie dostępu zespołowi

```
admin.microsoft.com → Users → Active users → wybieramy konto → Manage roles
→ Show all by category → Security Administrator (Security & Compliance) albo Security
Reader (Read-only) → Save changes
```

Izolację, zatwierdzanie akcji i zwalnianie z izolacji wykonuje Security Administrator. Security Reader tylko ogląda.

# Z życia wzięte

**Z ŻYCIA WZIĘTE**

Czwartek, 21:40. Kasia siedzi w hotelu w Gdańsku, a Defender zgłasza na jej laptopie alert o podejrzanym wierszu poleceń PowerShell z zakodowanym poleceniem. Dyżurny dostaje e-mail, wchodzi do kolejki incydentów i widzi, że system sam przeniósł plik do kwarantanny, ale

proces próbował jeszcze połączyć się z obcym adresem. Dyżurny izoluje laptop, dzwoni do Kasi i prosi o niezamykanie pokrywy, a jutro rano przejmuje sprawę z pełnym skanem i zmianą hasła.

# Jak to działa

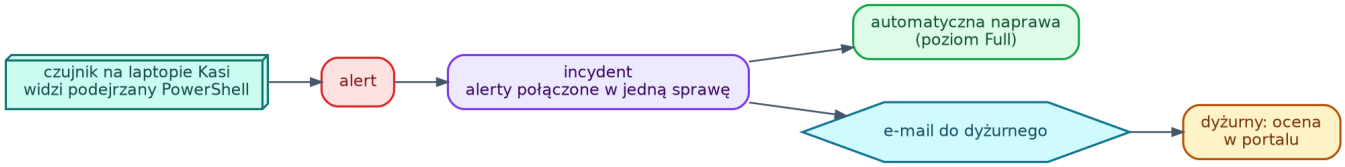
**Rozwiń: jak to działa pod spodem**

**Pojęcie: alert i incydent.** Alert to pojedyncze zgłoszenie czujnika o podejrzanym zdarzeniu. Incydent to zbiór powiązanych alertów, urządzeń i kont, połączonych w jedną sprawę, żeby dyżurny nie musiał układać ich ręcznie.

**Pojęcie: automatyczne dochodzenie i naprawa (AIR).** Mechanizm, który po wykryciu sam analizuje podejrzane obiekty i wykonuje działania naprawcze: kwarantanna pliku, zatrzymanie procesu, usunięcie zadania harmonogramu. W Defender for Business działa na poziomie pełnej automatyzacji, bez opcji zmiany. Od 1 września 2026 roku działa wewnątrz antywirusa i nie da się go uruchomić ręcznie. Do ręcznego sprawdzenia urządzenia służy pełny skan.

**Pojęcie: Action center.** Centralna lista działań naprawczych: oczekujących na zatwierdzenie i zakończonych, z możliwością cofnięcia. Tu widać i działania automatyczne, i ręczne, takie jak izolacja urządzenia albo skan.

**Pojęcie: automatic attack disruption.** Mechanizm wbudowany w Defender for Business: gdy wykryje atak prowadzony przez człowieka, sam izoluje urządzenie (contain device) i ogranicza konto użytkownika na tym urządzeniu. Tworzy incydent ze znacznikiem Attack Disruption. Zwolnienie: Release from containment albo Undo przy koncie. Wymaga, żeby wszystkie urządzenia firmy były dołączone do Defendera, a zwalnia go Security Administrator.




*Od czujnika na laptopie przez alert i incydent do automatycznej naprawy, e-maila i oceny dyżurnego (kliknięcie otwiera pełny rozmiar)*

# Co z EDR jest w Defender for Business

| Funkcja | W Business | Uwaga |
|---|---|---|
| Czujnik EDR i telemetria | tak | w wersji dla małych firm |
| Kolejka incydentów i alertów | tak | Incidents & alerts → Incidents |
| Automatyczna naprawa | tak, pełna automatyzacja | zintegrowana z antywirusem od 1 IX 2026 |
| Izolacja urządzenia | tak | pełna, wariant selektywny sprawdzamy w portalu |
| Skan antywirusowy z portalu | tak | szybki albo pełny |
| Wskaźniki blokowania i zezwalania | tak | Settings → Endpoints → Rules → Indicators |
| Zatrzymanie i kwarantanna pliku z portalu | niejednoznacznie | dokumentacja jest sprzeczna, sprawdzamy w portalu |
| Pakiet dochodzenia | nie wymieniony | akcja Planu 2 |
| Live response (zdalna powłoka) | nie | Plan 2 |
| Advanced hunting | nie | Plan 2 |
| Automatic attack disruption | tak | wbudowane, bez ustawień |

Skoro nie ma live response, wszystko, co robimy na urządzeniu, robimy przez użytkownika albo zdalny pulpit lub przez polecenia z tej strony.

# Wagi alertów

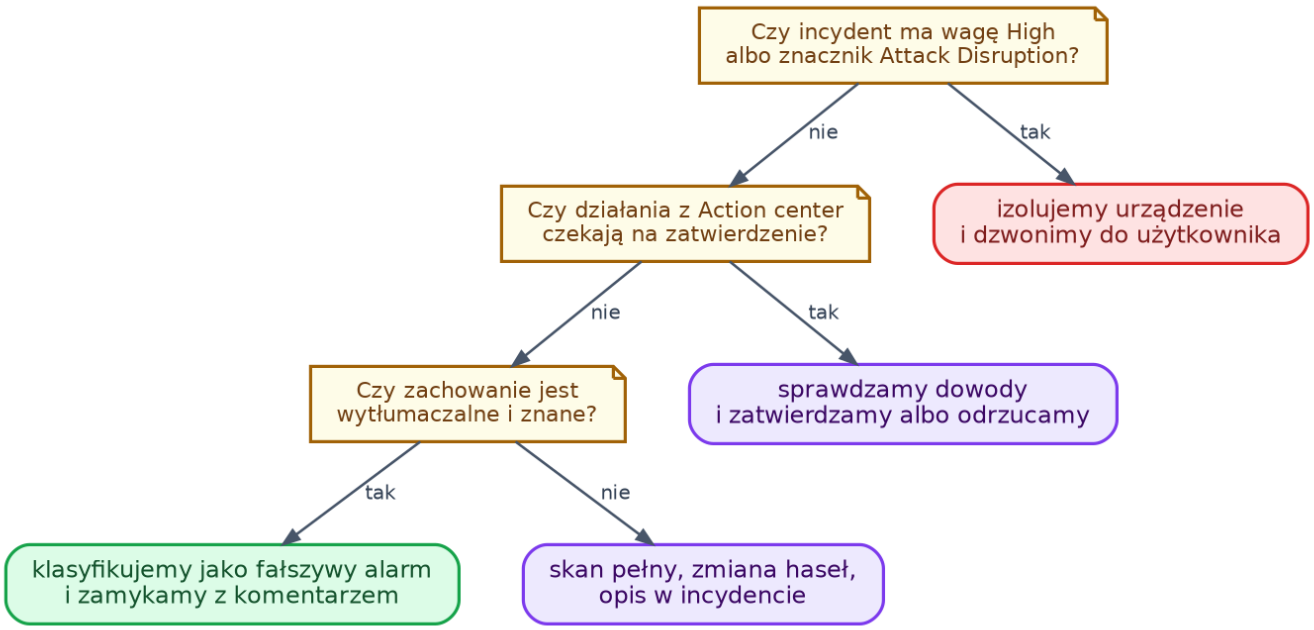
| Waga | Przykład | Domyślna reakcja Zielonej |
|---|---|---|
| High | wykryty zaawansowany atak (attack disruption) | izolacja i telefon w ciągu kwadransa |

| Waga | Przykład | Domyślna reakcja Zielonej |
|---|---|---|
| Medium | aktywne złośliwe oprogramowanie, zablokowane po chwili | sprawdzenie w ciągu godziny |
| Low | zagrożenie zatrzymane przed szkodą, podejrzane zachowanie bez wpływu na firmę | przegląd następnego dnia roboczego |
| Informational | zagrożenie zatrzymane, zanim cokolwiek zrobiło | tylko wgląd w raporcie |

Skala pochodzi z dokumentacji Business. Terminy w ostatniej kolumnie to nasza umowa w Zielonej, a nie reguła Microsoftu.

# Procedura dyżurnego Zielonej

1. Otwieramy e-mail z alertem i przechodzimy do Incidents & alerts → Incidents, zaczynając od wagi High, potem Medium.
2. Czytamy tytuł, urządzenie i konto. Sprawdzamy, kto używa urządzenia i czy użytkownik jest teraz w pracy, w terenie albo na VPN.
3. W Action center → Pending sprawdzamy, czy akcje czekają na zatwierdzenie. Oceniamy je i zatwierdzamy albo odrzucamy z komentarzem.
4. Przy wadze High albo znaczniku Attack Disruption izolujemy urządzenie i dzwonimy do użytkownika.
5. Uruchamiamy pełny skan z portalu i zapisujemy w incydencie, co zauważył czujnik.
6. Przy zakodowanym poleceniu odczytujemy je poleceniem z fiszki, zapisujemy domenę lub adres, z którym się łączy, i dodajemy wskaźnik blokowania.
7. Przy podejrzeniu przejęcia konta: reset hasła, unieważnienie sesji w Microsoft 365 i sprawdzenie logowań.
8. Klasyfikujemy incydent (prawdziwe zagrożenie albo fałszywy alarm), zamykamy go z komentarzem i zapisujemy, co zrobiono.
9. Gdy wykrycie było fałszywym alarmem, nie przywracamy pliku z kwarantanny bez weryfikacji, jak opisuje strona Utrzymanie i typowe problemy.




*Drzewo decyzji dyżurnego: waga High lub Attack Disruption prowadzi do izolacji, oczekujące akcje do zatwierdzenia, znane zachowanie do zamknięcia jako fałszywy alarm, a pozostałe do skanu i zmiany haseł (kliknięcie otwiera pełny rozmiar)*

# Scenka krok po kroku: zakodowany PowerShell na laptopie Kasi

Alert przychodzi o 21:40. W incydencie widać, że proces `powershell.exe` został uruchomiony z przełącznikiem `-EncodedCommand` przez program z archiwum pobranego z poczty. Defender przeniósł plik do kwarantanny, ale w Action center nie czeka nic do zatwierdzenia.

Dyżurny odczytuje polecenie komendą z fiszki. Okazuje się, że skrypt miał pobrać drugi plik z adresu `203.0.113.88` i uruchomić go w pamięci. Dyżurny dodaje ten adres jako wskaźnik blokowania, izoluje laptop i dzwoni do Kasi. Rano wykonuje pełny skan, zmienia hasło konta `kasia.nowak` i unieważnia jej sesje. Incydent zamyka z notatką: przyczyna, czas, podjęte kroki.

> Ta scenka zakłada, że kwarantanna i blokada zadziałały. Gdy skan lub log wskazuje, że drugi plik zdążył się uruchomić, nie czyścimy laptopa na własną rękę: przywracamy go z obrazu i zmieniamy hasła także w usługach, do których Kasia była zalogowana.

# Częste błędy

| Objaw | Przyczyna | Co robimy |
|---|---|---|
| Szukamy przycisku Initiate Automated Investigation | od 1 września 2026 roku ręczne uruchamianie usunięto | uruchamiamy pełny skan i patrzymy na Action center |
| Brak opcji live response | to funkcja Planu 2 | używamy skanu, izolacji i wskaźników, a zdalną diagnozę robimy zdalnym pulpitem |
| E-mail o alercie nie dochodzi do całego zespołu | reguły przypisane do osób, nie do grup | dodajemy reguły dla każdej osoby dyżurnej |
| Nie można zwolnić urządzenia z izolacji albo zatwierdzić akcji | konto ma rolę Security Reader | nadajemy Security Administrator |
| Użytkownik w terenie traci dostęp do wszystkiego po izolacji | pełna izolacja odcina sieć poza usługą Defender | uprzedzamy użytkownika telefonem i zwalniamy z izolacji po skanie |
| Incydent otwarty tygodniami | brak właściciela i klasyfikacji | każdy incydent klasyfikujemy i zamykamy z komentarzem |
| Zakodowane polecenie wklejone do konsoli i uruchomione | zbyt szybka próba zrozumienia | polecenie tylko odczytujemy, nie wykonujemy |

# □□ Ćwiczenia

1. W kolejce jest incydent z wagą Medium i jedną akcją w Action center → Pending. Co robimy w pierwszej kolejności?

**Odpowiedź**

Sprawdzamy, jaki obiekt Defender chce usunąć lub zatrzymać (plik, proces, zadanie harmonogramu), oceniamy, czy to zagrożenie, i zatwierdzamy albo odrzucamy akcję z komentarzem. Dopiero potem przechodzimy do skanu i klasyfikacji incydentu.

1. Dlaczego nie uruchamiamy zakodowanego polecenia z alertu, żeby zobaczyć, co robi?

**Odpowiedź**

Bo może wykonać dokładnie to, przed czym Defender chronił. Wystarczy je odczytać jako tekst funkcją dekodującą base64 i obejrzeć wynik w edytorze.

1. Czym różni się izolacja z portalu od automatic attack disruption?

**Odpowiedź**

Izolację wykonuje dyżurny ręcznie, gdy uzna to za potrzebne. Attack disruption działa automatycznie przy wykryciu ataku prowadzonego przez człowieka, izoluje urządzenie i ogranicza konto, tworzy incydent z odpowiednim znacznikiem, a zwolnienie jest ręczne.

**Powiązane:** Polityki ochrony: ochrona nowej generacji, zapora, reguły ASR i kontrolowany dostęp do folderów · Zarządzanie podatnościami i raporty: co łatać najpierw · Utrzymanie i typowe problemy · Antywirus, EDR, XDR, konsola zarządzania: cztery pojęcia

**Źródła:** Microsoft Learn, „View and manage incidents in Microsoft Defender for Business" · Microsoft Learn, „Respond to and mitigate threats in Microsoft Defender for Business" · Microsoft Learn, „Review remediation actions in the Action center" (Defender for Business) · Microsoft Learn, „Automatic attack disruption in Microsoft Defender for Business" · Microsoft Learn, „Take response actions on a device" (Defender for Endpoint) · Microsoft Learn, „Automated investigation and response changes" i „Automation levels" (Defender for Endpoint) · Microsoft Learn, „Set up email notifications in Microsoft Defender for Business" · Microsoft Learn, „Roles and permissions in Microsoft Defender for Business" · Microsoft Learn, „Review and edit settings in Microsoft Defender for Business" · Microsoft Learn, „Collect diagnostic data for Microsoft Defender Antivirus" · Microsoft Learn, „Live response in Microsoft Defender for Endpoint"

---

Revision #15
Created 2026-10-03 11:23:18 UTC by Tomasz Konieczny
Updated 2026-10-26 14:19:05 UTC by Tomasz Konieczny