

Bitdefender GravityZone EDR

System EDR (Endpoint Detection and Response) jest kluczową technologią, która zapewnia ciągłe monitorowanie sieci w celu wykrywania i reagowania na cyberzagrożenia. W obliczu rosnących zaawansowanych ataków cybernetycznych, system EDR zapewnia szybkie wykrywanie podejrzanej aktywności i pomaga w minimalizowaniu ryzyka naruszenia bezpieczeństwa danych.

Dzięki rozwiązaniu Bitdefender GravityZone EDR organizacje mogą skutecznie zabezpieczać swoje infrastruktury przed najbardziej wyrafinowanymi atakami.

Dlaczego Bitdefender GravityZone EDR?

Bitdefender GravityZone EDR to kompleksowe rozwiązanie, które zapewnia nie tylko ochronę przed tradycyjnymi zagrożeniami, ale także skutecznie radzi sobie z najnowszymi, zaawansowanymi atakami cybernetycznymi. Dzięki zaawansowanej technologii wykrywania i reagowania na zagrożenia, organizacje mogą szybciej identyfikować incydenty i natychmiastowo na nie reagować. Platforma ta łączy zaawansowane funkcje EDR z rozbudowanym systemem XDR, oferując wyjątkową efektywność w zarządzaniu bezpieczeństwem punktów końcowych, a także zwiększoną automatyzację i uproszczenie procesów obronnych.

**Zmniejsz wysiłki i koszty
związane z bezpieczeństwem**

90%

Zmniejsz wysiłki związane z bezpieczeństwem nawet o 90%, konsolidując i automatyzując zabezpieczenia wykraczające poza EDR dzięki najbardziej kompleksowej ochronie punktów końcowych i platformie rozszerzonego wykrywania i reagowania (XDR).

**Przyspiesz reakcje na incydenty
w punktach końcowych**

50%

Przyspiesz reakcję na incydenty o 50% dzięki automatycznej korelacji między punktami końcowymi, praktycznym wnioskowi na temat incydentów i prostym rekomendacjom dotyczącym reakcji, wspierając zespoły dowolnej wielkości i poziomu doświadczenia.

**Zapobiegaj atakom i zatrzymuj
je wcześniej**

85%

Zmniejsz liczbę incydentów nawet o 85% dzięki rozwiązaniom zabezpieczającym, które zostały opracowane z myślą o zapobieganiu i niezmiennie zajmują pierwsze miejsce w niezależnych ocenach skuteczności zapobiegania i wykrywania.

Zatrzymaj ransomware i zaawansowane ataki dużo szybciej, przy mniejszym wysiłku!

Lider w dziedzinie bezpieczeństwa punktów końcowych

Bitdefender XDR został doceniony przez ekspertów do spraw cyberbezpieczeństwa z Forrester Wave™ i zaliczono go do **mocnych dostawców platform rozszerzonego wykrywania i reagowania w teście z drugiego kwartału 2024**. Konsekwentnie wykazuje najwyższą wydajność w zaufanych testach organizacji takich jak Gartner, MITRE, AV-Comparatives lub AV-TEST.

Kompleksowa platforma EPP i XDR

Platforma GravityZone zapewnia kompleksowe zarządzanie ryzykiem, zapobieganie, ochronę oraz rozszerzone wykrywanie i reagowanie, konsolidując dochodzenia w punktach końcowych, tożsamościach, aplikacjach produkcyjnych, sieci, chmurach, urządzeniach mobilnych i nie tylko.

Wysoce zautomatyzowany i intuicyjny

Przebieg pracy dochodzeniowej są usprawniane przez GravityZone EDR dzięki automatycznej korelacji między punktami końcowymi, wysoce dokładnej zautomatyzowanej ochronie, intuicyjnym wizualizacjom i rekomendacjom odpowiedzi.

Zalety Bitdefender GravityZone EDR z przykładami.

1. Zarządzanie z poziomu jednej centralnej konsoli administracyjnej.

Zaletą Bitdefender EDR jest fakt, że zarządzamy nim z poziomu **jednej konsoli administracyjnej, która jest dostępna w języku polskim**. Instalacja Bitdefender EDR jest także prosta i intuicyjna:

- ↳ po założeniu konta i aktywacji licencji **zakładka Incydenty** odpowiadająca za EDR jest od razu dostępna.
- ↳ Nie trzeba otwierać osobnej konsoli czy też czekać na aktywację.

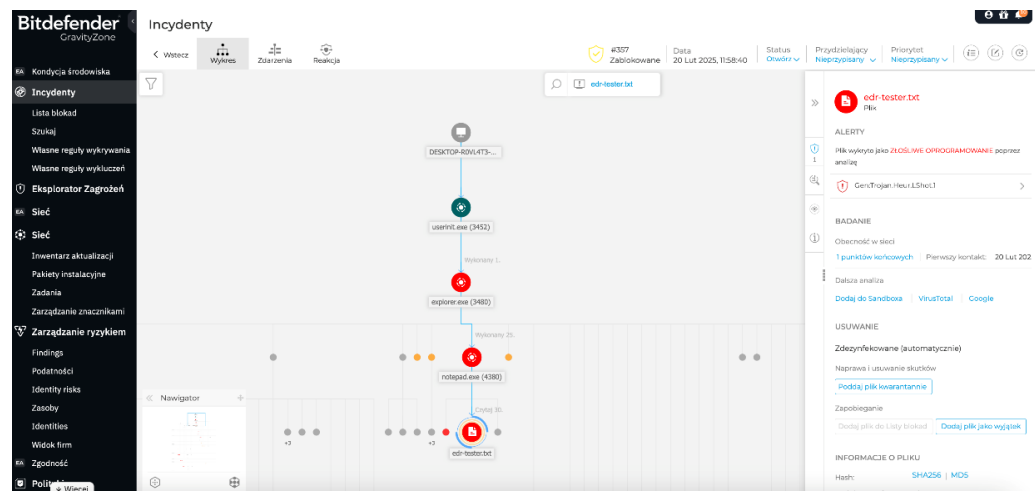
ID	Status	Utworzono	Ostatnia aktualizacja	Według stanu	Ocena s...	Przydzielający	Priorytet	Firma	Podmioty	Zasoby
#DEMO	Otworzono	15 Sep 2023, 14:01	15 Sep 2023, 14:01	Otworz...	88	Nieprzydzielony	Nieprzy...	Demo Company	desktop-rb...	-
#357	Otworzono	20 Feb 2025, 11:58	20 Feb 2025, 12:31	Otworz...	48	Nieprzydzielony	Nieprzy...	Marken Ultra	desktop-rb...	-
#356	Otworzono	16 Dec 2024, 09:00	16 Dec 2024, 09:07	Otworz...	50	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest1-000c...	-
#355	Otworzono	10 Dec 2024, 10:03	10 Dec 2024, 10:07	Otworz...	50	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest1-000c...	-
#354	Otworzono	27 Nov 2024, 18:18	27 Nov 2024, 18:18	Otworz...	74	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest1-000c...	-
#353	Otworzono	21 Nov 2024, 08:22	21 Nov 2024, 08:24	Otworz...	48	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest2-000c...	-
#352	Otworzono	21 Nov 2024, 08:22	21 Nov 2024, 08:23	Otworz...	54	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest2-000c...	-
#351	Otworzono	21 Nov 2024, 08:19	21 Nov 2024, 08:21	Otworz...	63	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest2-000c...	-
#350	Otworzono	21 Nov 2024, 08:19	21 Nov 2024, 08:19	Otworz...	44	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest2-000c...	-
#349	Otworzono	21 Nov 2024, 08:16	21 Nov 2024, 08:17	Otworz...	48	Nieprzydzielony	Nieprzy...	Marken Ultra	pctest2-000c...	-

W Bitdefender EDR mamy możliwość natychmiastowego zarządzania incydentami EDR z poziomu jednej centralnej konsoli.

2. Czytelność incydentów

Incidenty często przedstawiane są jako sieć połączeń, która jest trudna do zrozumienia dla użytkownika. Dlatego **incydenty w Bitdefender EDR przedstawione są z góry na dół**:

- ↳ na samej górze widnieje punkt końcowy, na którym wystąpił incydent,
- ↳ schodząc w dół widzimy natomiast po kolei pliki lub procesy zaangażowane w ten incydent.



Czytelność i prostota w przedstawieniu incydentów usprawnia i ułatwia ich analizę.

3. Proste tworzenie własnych reguł wykrywania

Często zdarza się, że tworzenie własnych reguł po spełnieniu, których zostanie wygenerowany incydent wymaga znajomości kodu lub wyszukiwania składni w dokumentacji oraz pisania własnych zapytań.

↳ Tworzenie własnych reguł w Bitdefender EDR odbywa się w trybie graficznym z wykorzystaniem operatorów logicznych.

Prostota w tworzeniu własnych reguł, po spełnieniu których zostanie wygenerowany incydent

4. Skuteczność działania

Bitdefender EDR ma udowodnioną skuteczność. Dla testu na maszynie wirtualnej została podjęta próba uruchomienia złośliwego skryptu mającego za zadanie testować działanie EDR.

↳ Może zdarzyć się, że system EDR pozwoli na zapisanie skryptu do pliku .txt, zmianę rozszerzenia pliku na .bat oraz ostatecznie umożliwi uruchomienie próbki. Dopiero po uruchomieniu próbki zacznie na bieżąco blokować poszczególne komendy zawarte w skrypcie.

↳ **Bitdefender EDR natychmiastowo zablokował zapis skryptu do pliku .txt oraz uniemożliwił zmianę rozszerzenia pliku**- zmiana rozszerzenia wymagała wyłączenia ochrony. Po zmianie rozszerzenia na .bat **Bitdefender EDR nie pozwolił także uruchomić próbki**.

Incident Bitdefender EDR kończy się już na etapie pliku .txt, co potwierdza jego skuteczność.

5. Tworzenie własnych reguł blokowania

Bitdefender EDR pozwala na dodanie do listy blokowanych **hash, ścieżkę aplikacji lub dodanie konkretnego połączenia**.

↳ **Bitdefender EDR posiada wiele możliwości tworzenia własnych reguł blokowania**

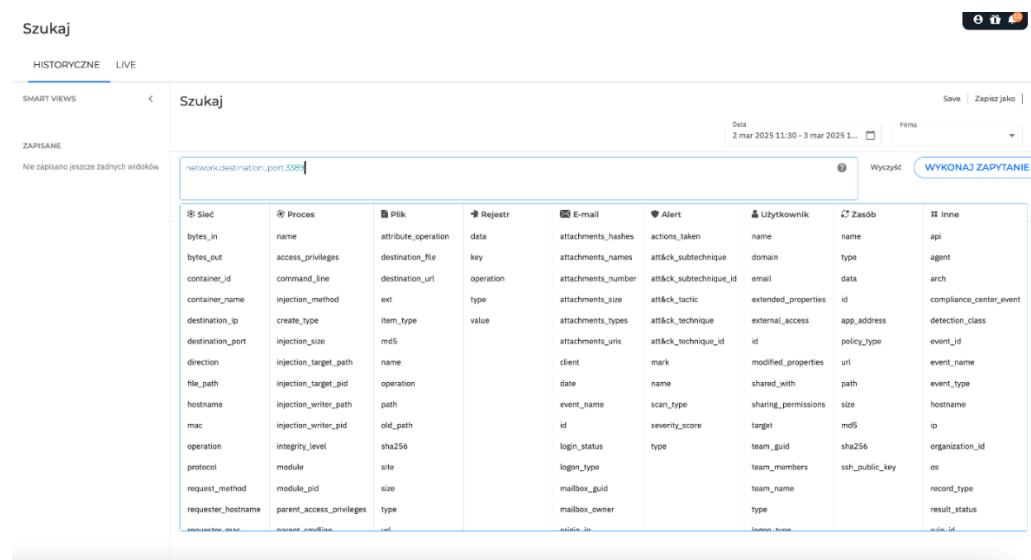
6. Wyszukiwanie zdarzeń

Wyszukiwanie incydentów często wymaga pisania zapytań od zera, podobnych do tych podczas tworzenia własnych reguł wykrywania. Użytkownik musi znać odpowiednie zmienne lub szukać ich w dokumentacji.

Wyszukiwanie w Bitdefender EDR udostępnia zapytania pogrupowane na kategorie, które możemy następnie uzupełniać własnymi danymi.

Wyszukiwanie w Bitdefender EDR udostępnia zapytania pogrupowane na kategorie, które możemy następnie tylko uzupełniać własnymi wartościami.

➤ **Przykład:** Po kliknięciu w pozycję **destination port** w kolumnie **Sieć** kod uzupełni się automatycznie. Następnie po dwukropku wystarczy podać tylko numer portu, dla którego połączenia chcemy wyszukać.

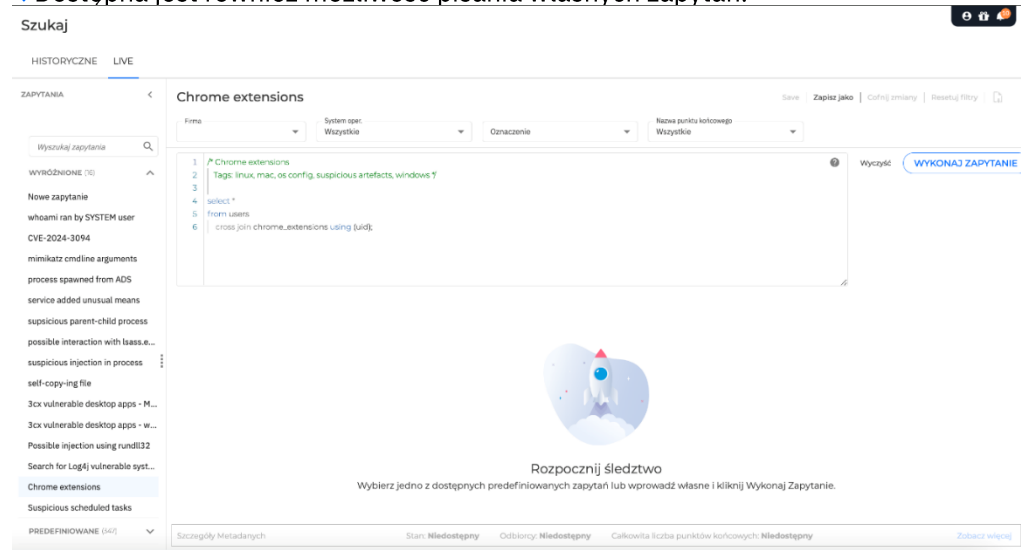


Bitdefender EDR to zatem większa prostota w obsłudze mechanizmu wyszukiwania incydentów.

7. Odpytywanie punktów końcowych

Bitdefender EDR umożliwia odpytywanie aktywnych punktów końcowych pod kątem prawie 350 gotowych zapytań.

➤ Dostępna jest również możliwość pisania własnych zapytań.



W celu uzyskania więcej informacji prosimy o kontakt z opiekunem handlowym lub