DATASHEET

Bitdefender

MDR

Usługa Bitdefender Managed Detection & Response

POPRAW SWOJE WYNIKI W ZAKRESIE BEZPIECZEŃSTWA DZIĘKI MANAGED DETECTION AND RESPONSE

Wielu z naszych klientów ma problemy z ochroną swoich firm w obliczu narastająco złożonych i mutujących środowisk technologicznych i coraz bardziej wyszukanych ataków, Usługa Bitdefender Managed Detection and Response łączy nasze nagradzane silniki EDR z nowoczesną operacją bezpieczeństwa działającą 24/7 obsadzoną światowej klasy doświadczeniem w celu wyszukiwania, identyfikowania i usuwania atakujących.

Współczesne wyzwania dla bezpieczeństwa organizacji

Zagrożenie i znaczenie zabezpieczeń dla firm na całym świecie ciągle wzrasta. Ataki stają się coraz bardziej wyszukane i odporne na typowe metody zapobiegania. Firmy muszą dostosować strategie i zasoby w kierunku szybkiego i efektywnego identyfikowania wycieków i szybkiego reagowania. Według przeprowadzonych w 2019 badań Accenture “Cost of Cybercrime”, średni koszt cyber incydentów dla firm wzrósł o 72% przez ostatnie 5 lat do 31 milionów dolarów podczas gdy liczba wycieków wzrosła o 67% w tym samym okresie.

W 2019 raport Data Breach Investigations Report (DBIR) od Verizon, wykazał, że laptopy i komputery odpowiadały za około 25% zasobów w wyciekach danych. Użytkownicy tych urządzeń są bezpośrednim celem atakujących dzięki wykorzystaniu inżynierii społecznej takiej jak Phishing, który odpowiadał za 33% wycieków, wzrost o 18 punktów z wyników z 2017. W rezultacie krytycznym jest skupienie się na pracownikach i ich urządzeniach, ponieważ są najczęstszym pierwszym krokiem w schemacie ataku.

Coraz więcej klientów zdaje sobie sprawę z wagi zabezpieczeń w ich firmach i podatności ich systemów. Większości z nich brakuje zasobów do przeprowadzenia operacji zdolnej do wykrywania i reagowania na wyszukane i popularne zagrożenia. Według Verizon 2019 DBIR, 56% wycieków zostało wykrytych po miesiącach podczas gdy fazy Compromise and Exfiltration atakujących są mierzone od minut do dni.

W jaki sposób usługa Managed Detection & Response Bitdefendera pomaga?

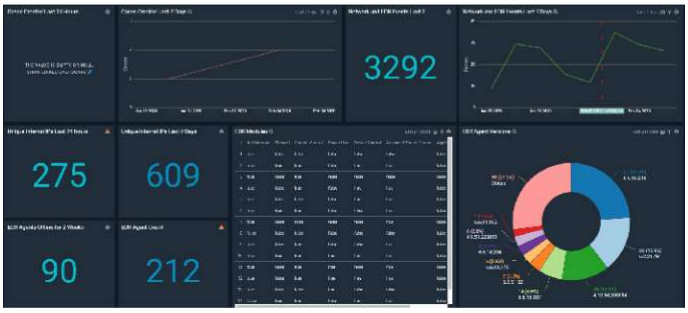
Usługa Managed Detection & Response Bitdefendera rozpoczyna się od naszej nagradzanej platformy technologicznej, którą nazywamy potrójnym stosem – punkty końcowe, sieć i analityka bezpieczeństwa. Dla widoczności sieci i punktów końcowych używamy platformy ochrony Bitdefender GravityZone Ultra w parze z Bitdefender Network Traffic Security Analytics. Te dane są przesyłane do naszej platformy analitycznej.

Ta telemetria jest wykorzystywana do generowania alertów dzięki narzędziom bezpośredniej detekcji, maszynowemu uczeniu i wyszukiwaniu zagrożeń. Nasze proaktywne wyszukiwanie zagrożeń wykorzystuje strategiczne threat intelligence do tworzenia misji poszukiwawczych, które są wykonywane przez naszych analityków do wykrywania wyrafinowanych atakujących, którzy mogą zostać niewykryci przez inne narzędzia.

Nasz zespół ds. operacji bezpieczeństwa zbada i zareaguje na każdy wygenerowany incydent przez narzędzia lub podczas naszego poszukiwania zagrożeń przez zestaw wstępnie zatwierdzonych akcji.

Akcje są szczegółowe i zatwierdzone przez twój zespół podczas wdrożenia dzięki czemu możemy je szybko wykonać aby przechwycić atakujących zanim narobią szkód w twojej firmie,

Klienci otrzymują informacje w czasie rzeczywistym na temat statusu operacji, podsumowujące raporty pokazujące zbiorcze dane z historycznymi trendami i raporty po akcji, które zawierają wszystkie szczegóły incydentu i działanie podjęte w celu jego usunięcia.



Funkcje & Korzyści

Endpoint Detection / Prevention

Światowej klasy technologia punktów końcowych, zapobieganie znanym zagrożeniom i dostarczanie danych analitykom bezpieczeństwa w celu identyfikowania zaawansowanych ataków i poprzednio nieznanych zagrożeń.

Threat Intel

Zapewnianie wglądu w branżę i tworzenie misji wyszukiwania zagrożeń

Analiza Ruchu Sieciowego

Monitorowanie sieci i urządzeń, które nie są objęte technologią agenta punktów końcowych (IoT, drukarki, BYOD itp.)

Wstępnie zatwierdzone akcje

Izolacja i eliminacja zagrożeń w czasie rzeczywistym, ograniczanie czasu przebywania i przechodzenia przez sieć

Technical Account Management

TAM zapewnienia dedykowane wsparcie i kwartalne przeglądy

Analiza Malware

Analiza automatyczna i na żądanie podejrzanego oprogramowania