

Analitycy zajmujący się bezpieczeństwem wskazują, że największym wyzwaniem jest dziś bycie na bieżąco ze stale zmieniającymi się metodami cyberataków. Niedawno przeprowadzone badanie IBM pokazuje, że obecnie zaledwie 7% specjalistów korzysta w swojej pracy z narzędzi kognitywnych, ale w najbliższych 2-3 latach ta liczba może wzrosnąć nawet trzykrotnie.

Narzędzie, które IBM przygotowało, aby pomóc w uzupełnieniu wiedzy oraz szybszym, bardziej precyzyjnym reagowaniu to platforma IBM Cognitive Security Operations Center. Aplikacja IBM QRadar Watson Advisor asystuje w badaniu zagrożeń, skanując blogi, strony internetowe i publikacje naukowe przy wykorzystaniu możliwości przetwarzania języka naturalnego oraz zestawia je z danymi QRadar, pokazującymi ujawnione incydenty bezpieczeństwa.

Dzięki temu czas potrzebny na zdefiniowanie zagrożenia skraca się z kilku godzin do kilku minut.

Rozwiązanie Watson for Cyber Security zostanie zintegrowane w ramach nowej platformy IBM Cognitive SOC, pozwalającej na identyfikowanie i reagowanie na zdarzenia na urządzeniach końcowych, w sieci, na kontach użytkowników oraz w chmurze obliczeniowej. Sercem platformy jest IBM QRadar Watson Advisor, nowa aplikacja zapewniająca dostęp do wiedzy o zagrożeniach w cyberprzestrzeni. Aplikacja jest już dziś używana, między innymi, przez firmę Uniwersytet w New Brunswick oraz 40 innych klientów z całego świata i pozwala analitykom na lepszy wgląd w incydenty związane z bezpieczeństwem.

„IBM Cognitive SOC wspiera klientów w walce z rosnącą liczbą zagrożeń płynących z sieci” – mówi Marcin Spychała, ekspert ds. bezpieczeństwa w IBM. „Inwestycje w technologię kognitywną Watson w obszarze cyberbezpieczeństwa pozwoliły nam rozwinąć kilka innowacji w ciągu zaledwie 12 miesięcy. Wierzimy, że właśnie połączenie wiedzy specjalistów zajmujących się cyfrowymi zagrożeniami i możliwości sztucznej inteligencji będzie tym, co zdefiniuje walkę z przestępczością online w przyszłości”.

Ochrona urządzeń końcowych jest jednym z ważniejszych obszarów w systemie ochrony przed cyberatakami. Dlatego IBM wprowadza BigFix Detect, rozwiązanie pozwalające organizacjom na wgląd i natychmiastową reakcję w urządzeniu z poziomu platformy. Pozwoli to na szybsze dochodzenie i lepsze zrozumienie natury i rodzaju zagrożenia, a w połączeniu z innymi technologiami IBM – na przykład i2 czy IBM X-Force Exchange – na bardziej zautomatyzowane, a przez to dokładniejsze reakcje.