Bitdefender

Sztuczna inteligencja w cyberbezpieczeństwie: czy sama automatyzacja może zabezpieczyć Twoją organizację?

17.10.2024

W miarę jak sztuczna inteligencja (AI) ewoluuje, a organizacje stają się coraz bardziej zależne od automatyzacji, specjaliści ds. cyberbezpieczeństwa będą musieli upewnić się, że nie staną się zbyt zależni od technologii. Obecność człowieka w pętli zapewnia, że AI zachowuje się w oczekiwany sposób, aby uniemożliwić złośliwym aktorom penetrację krytycznych systemów biznesowych bez wprowadzania dodatkowego ryzyka dla organizacji. Jeśli istnieje granica między zbyt dużym a zbyt małym poleganiem na AI, gdzie ona jest i jak ją utrzymać w sposób, który przynosi wartość bez wprowadzania większego ryzyka?

Sztuczna inteligencja zmienia cyberbezpieczeństwo po obu stronach

AI i uczenie maszynowe (ML) przekształciły cyberbezpieczeństwo w ciągu ostatnich kilku lat. Eksplozja powierzchni zagrożeń spowodowana transformacją cyfrową, przetwarzaniem w chmurze i hybrydowymi modelami pracy wprowadziła ogromną złożoność w obszarze bezpieczeństwa. Organizacje polegają teraz na dziesiątkach narzędzi bezpieczeństwa, aby monitorować tę rozszerzającą się powierzchnię zagrożeń, co prowadzi do zmęczenia alertami i wypalenia, które utrudniają cybergotowość.

AI może zautomatyzować wiele z tych żmudnych zadań, usprawnić przepływy pracy związane z bezpieczeństwem i zapewnić odpowiedni kontekst wokół zdarzeń i incydentów. Upraszcza to operacje związane z bezpieczeństwem, zapewnia spójność w całym środowisku IT i uwalnia zasoby ludzkie do zadań wymagających myślenia na wyższym poziomie.

Nie ma już potrzeby ścigania każdego fałszywego alarmu ani monitorowania dzienników zdarzeń w nocy i w weekendy. AI stała się na tyle inteligentna, aby identyfikować zdarzenia wymagające dodatkowej uwagi, zapewniać odpowiedni kontekst i formułować zalecenia, które ludzie mogą wykonać lub, w niektórych przypadkach, pozwalać AI na automatyczne wyzwalanie działań.

Problem polega na tym, że dzisiejsi cyberprzestępcy również używają AI do ulepszania taktyk i technik, których używają do infiltracji sieci przedsiębiorstw. Wiedzą, że eksperci do spraw cyberbezpieczeństwa są przytłoczeni i polegają na AI w celu automatyzacji powtarzających się zadań, i mogą wykorzystać tę wiedzę, aby odpowiednio dostosować

swoje taktyki. Zestawy narzędzi phishingowych, trwałe narzędzia, powłoki malware i ataki bezplikowe są zaprojektowane tak, aby unikać tradycyjnych rozwiązań bezpieczeństwa i zaciemniać ich działania wokół legalnego zachowania, nie pozostawiając prawie żadnego podpisu, z którego AI mogłaby się uczyć i identyfikować w przyszłości.

Nadmierne poleganie na sztucznej inteligencji wzmacnia samozadowolenie zespołów ds. cyberbezpieczeństwa i ułatwia atakującym ukrywanie się na widoku.

Utrzymywanie kontaktu z człowiekiem jest niezbędne, aby zachować równowagę

Tesla może być w stanie prowadzić się sama, ale do jej podłączenia nadal potrzebny jest człowiek. To samo można powiedzieć o cyberbezpieczeństwie. AI może przejąć wiele ciężkich zadań od analityków bezpieczeństwa, ale musi być człowiek w pętli, aby stale szkolić, aktualizować i monitorować te narzędzia – zwłaszcza, aby nadążać za ciągle zmieniającym się krajobrazem zagrożeń. Ważne jest, aby pamiętać, że AI jest tylko narzędziem, którego celem jest wspomaganie działań człowieka.

AI jest tak dobra, jak dane, które ludzie do niej wprowadzają. Analitycy powinni stale aktualizować i szkolić swoje modele za pomocą najnowszych informacji o zagrożeniach, a także zmian w cyfrowej infrastrukturze swojej organizacji i zachowaniach użytkowników. Dzięki temu ludzie mogą być o krok przed swoimi złośliwymi odpowiednikami, tworzyć aktualne podręczniki odpowiedzi i pozwalać AI analizować

wyniki i formułować zalecenia, gdy podejmowane są próby infiltracji systemów. Wiedza, kiedy pozwolić AI robić swoje, a kiedy interweniować, to nauka. Użytkownicy muszą zrozumieć możliwości AI, jej ograniczenia i jak najlepiej wykorzystać to narzędzie. Ostatecznie to ludzie muszą kierować strategią i pozwolić maszynom ją realizować.

„Oczywiście, istnieje narzędzie, które pomaga zarządzać możliwościami AI i utrzymać zgodność narzędzi AI zgodnie z aktualnymi zasadami bezpieczeństwa. Rozwiązania Extended Detection and Response (XDR) pozwalają na inwentaryzację zasobów IT, monitorowanie ich zachowania w czasie rzeczywistym, a także ocenę podatności i zagrożeń dla organizacji. Rozwiązania XDR mogą analizować duże ilości danych i dostarczać rekomendacji dotyczących usuwania podatności w zabezpieczeniach i naprawiania skutków ataków. Jednak XDR to nadal narzędzie, które wymaga czynnika ludzkiego, aby wykorzystać je w jak najbardziej optymalny sposób" – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora Bitdefender.

Oprócz XDR, centra operacji bezpieczeństwa (SOC) odgrywają kluczową rolę w zapewnianiu całodobowego monitorowania i obrony przed zagrożeniami cybernetycznymi. SOC zapewniają wiedzę specjalistyczną potrzebną do interpretowania złożonych danych, reagowania na incydenty w czasie rzeczywistym i ciągłego dostosowywania obrony do zmieniającego się krajobrazu zagrożeń.

Usługi Managed Detection and Response (MDR) mogą rozszerzyć tę możliwość, oferując organizacjom ciągłe polowanie na zagrożenia, monitorowanie i reagowanie na incydenty za pośrednictwem globalnych

SOC. Ta kombinacja narzędzi opartych na sztucznej inteligencji i ludzkiej inteligencji pozwala organizacjom utrzymać skuteczną i zwinną postawę cyberbezpieczeństwa, zapewniając, że żadne krytyczne alerty nie zostaną pominięte i umożliwiając szybką naprawę po wykryciu zagrożeń.

Pozostać o krok przed konkurencją

AI przekształca przestrzeń cyberbezpieczeństwa zarówno dla obrońców, jak i atakujących. AI automatyzuje żmudne zadania na dużą skalę, poprawia postawę bezpieczeństwa, tworzy wydajność operacyjną i uwalnia zasoby ludzkie do zadań wymagających myślenia na wyższym poziomie. Jednak nadmierne poleganie na możliwościach AI może spowodować opieszałość wśród pracowników cyberbezpieczeństwa i pozwalać cyberprzestępcom wyjść o krok do przodu, narażając organizację na duże ryzyko. Człowiek musi być na bieżąco ze wszystkimi rozwiązaniami AI, stale szkoląc modele, aby nadążać za zmieniającym się krajobrazem zagrożeń, zapewniając jednocześnie oczekiwane rezultaty.

Wymaga to świadomości środowiska IT, potencjalnych luk w zabezpieczeniach oraz najnowszych taktyk i technik zagrożeń. Rozwiązania XDR mogą zapewnić tę świadomość w czasie rzeczywistym, umożliwiając maksymalne wykorzystanie rozwiązań cyberbezpieczeństwa opartych na AI bez narażania organizacji na ryzyko.

Źródło:https://bitdefender.pl/sztuczna-inteligencja-w-cyberbezpieczenstwie-czy-sama-automatyzacja-moze-zabezpieczyc-

twoja-organizacje/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 17.10.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.