LISTA KONTROLNA

11 porad dotyczących wdrożenia GenAI w operacje bezpieczeństwa

Generatywna sztuczna inteligencja (GenAI) oferuje niespotykane dotąd możliwości poprawy operacji bezpieczeństwa (SecOps). Integracja GenAI z platformą cyberbezpieczeństwa znacząco upraszcza identyfikacje zagrożeń i pomaga zniwelować lukę kompetencyjną w obszarze cyberbezpieczeństwa. Aby sprawnie ocenić i włączyć GenAI w SecOps, warto podjąć poniższe kroki.

☑ Udokumentuj przypadki użycia GenAI

Utwórz szczegółowy wykaz wszystkich planowanych zastosowań GenAI w swojej organizacji. Znajdź ewentualne luki w zabezpieczeniach związane z prywatnością i ochroną danych oraz zgodnością z przepisami. Opracuj kompleksowy dokument oceny ryzyka, który szczegółowo opisuje te zagrożenia oraz strategie ich minimalizacji. Dokument ten stanowi solidny fundament dla inicjatyw związanych z GenAI i pomaga zapewnić bezpieczne wdrożenia.

☑ Zrozum zasady zarządzania danymi AI

Właściwe zarządzanie danymi jest kluczem do pomyślnych wyników stosowania GenAI w SecOps, w związku z czym należy dokumentować typy danych, z których będą korzystać systemy AI. Uwzględnij ich źródła, techniki przetwarzania oraz metody przechowywania. Zrozumienie tych aspektów pomaga ustalić jasne zasady dotyczące wykorzystania danych i zapewnić zgodność z odpowiednimi standardami bezpieczeństwa oraz przepisami dotyczącymi prywatności danych. Wdrożenie ścisłej klasyfikacji danych może dodatkowo przyczyniać się do efektywnego zarządzania danymi AI oraz ich ochrony.

☑ Oceń zewnętrzne czynniki ryzyka związane z GenAI

Ocena zewnętrznych czynników ryzyka związanych z GenAI obejmuje ustalenie, jak usługi AI firm zewnętrznych mogą wpływać na Twoją organizację. Warto rozważyć takie sytuacje jak przetwarzanie danych przy użyciu zewnętrznych narzędzi wspomaganych przez sztuczną inteligencję i związane z nimi potencjalne zagrożenia. Odpowiedzi na te pytania pomogą opracować kompleksową strategię zarządzania ryzykiem, chroniąc organizację przed zagrożeniami zewnętrznymi i zapewnić bezpieczną integrację technologii GenAI.

☑ Sporządź listę zatwierdzonych narzędzi GenAI

Wybranie odpowiednich narzędzi GenAI jest wprost niezbędne do ich bezpiecznego i efektywnego wdrożenia. Oceń każde narzędzie pod względem jego funkcji ochrony, zgodności z przepisami dotyczącymi prywatności i możliwości integracji z istniejącymi systemami. Należy też wziąć pod uwagę takie aspekty jak koszt i łatwość użytkowania. Po zidentyfikowaniu najbardziej odpowiednich narzędzi sporządź listę zatwierdzonych usług GenAI i upewnij się, że informacje te są jasno przekazywane w ramach organizacji.

☑ Opracuj politykę dotyczącą GenAI

Kompleksowa polityka dotycząca GenAI stanowi fundament jej etycznego i praktycznego użytkowania. Polityka ta powinny określać standardy bezpiecznego wdrożenia GenAI, w tym wytyczne dotyczące przejrzystości i odpowiedzialności. Zadbaj, by wszyscy pracownicy znali swoje obowiązki i oczekiwania związane z korzystaniem z GenAI. Regularne aktualizacje tej polityki pomogą swobodnie nadążać za stale rozwijanymi technologiami i zagrożeniami.

☑ Zintegruj GenAI z używaną infrastrukturą

Płynna integracja możliwości GenAI z używanymi narzędziami do ochrony i procesami pracy ma krytyczne znaczenie z perspektywy maksymalizacji korzyści. Aby zwiększyć ogólną efektywność, należy skupić się na osadzeniu GenAI w istniejących centralnych narzędziach do zarządzania danymi i analizami, systemach zarządzania informacjami i zdarzeniami z zakresu bezpieczeństwa oraz platformach orkiestracji, automatyzacji i reagowania związanych z ochroną. Opracuj jasne procedury, które posłużą analitykom jako zasady przewodnie w interakcjach z GenAI, umożliwiając im efektywne korzystanie z możliwości tej technologii bez zakłócania obecnych procesów.

☑ Zadbaj o przeszkolenie pracowników zajmujących się bezpieczeństwem

Zapewnij zespołowi ds. bezpieczeństwa kompleksowe szkolenie w zakresie skutecznego korzystania z narzędzi GenAI. Upewnij się, że szkolenie obejmuje możliwości i ograniczenia GenAI oraz opracuj najlepsze praktyki wykorzystania tej technologii w codziennych operacjach. Szkolenie pomaga zadbać, aby zespół był dobrze przygotowany do integracji GenAI ze swoimi przepływami pracy i potrafił zmaksymalizować jej potencjał przy jednoczesnym zminimalizowaniu ryzyka.

☑ Zautomatyzuj rutynowe zadania

Automatyzacja powtarzalnych zadań za pomocą GenAI może znacznie zwiększyć efektywność SecOps. Zidentyfikuj zadania — takie jak korelacja danych, generowanie raportów czy wstępne oceny zagrożeń — które można zautomatyzować. Automatyzacja ta pozwoli analitykom skupić się na bardziej złożonych i strategicznych kwestiach, zwiększających produktywność pracy i efektywność operacyjną. Obniży to też ryzyko błędu człowieka w tych rutynowych zadaniach, a zarazem poprawi ogólny stan bezpieczeństwa środowiska.

☑ Usprawnij badanie zagrożeń i reagowanie na nie

GenAI może zrewolucjonizować procesy badania zagrożeń i reagowania na nie. Można się nią posłużyć w celu analizowania alertów i incydentów, generowania kompleksowych podsumowań eskalacji oraz korelowania danych z wielu źródeł. Te możliwości pozwolą na szybsze i bardziej precyzyjne wykrywanie zagrożeń oraz odpowiedź na nie. Dzięki GenAI zespół może sprawniej i skuteczniej reagować na incydenty, ograniczając negatywne skutki ewentualnego naruszenia zabezpieczeń.

☑ Zoptymalizuj wskaźniki wydajności

Monitorowanie i optymalizacja kluczowych wskaźników wydajności, takich jak średni czas wykrycia czy średni czas reakcji, ma zasadnicze znaczenie z perspektywy oceny skuteczności wdrożenia GenAI. Stale dokonuj ocen wpływu GenAI na te wskaźniki i dostosowuj swoje strategie tak, aby poprawiać skuteczność i zapewniać niezawodność operacji związanych z bezpieczeństwem. Regularne przeglądanie tych wskaźników pomoże Ci wykryć obszary wymagające poprawy i upewnić się, że integracja GenAI przynosi oczekiwane korzyści.

☑ Dbaj o przejrzystość i odpowiedzialność

Opracowanie i egzekwowanie polityki etycznego użytkowania GenAI ma kluczowe znaczenie z perspektywy utrzymywania zaufania oraz odpowiedzialności. Zadbaj o przejrzystość decyzji i działań opartych na sztucznej inteligencji oraz wdróż mechanizmy monitorowania i weryfikowania wyników uzyskiwanych za pomocą sztucznej inteligencji. Praktyki te budują zaufanie w organizacji i wzmacniają poczucie rzetelności operacji związanych z bezpieczeństwem. Regularne audyty i przeglądy pomagają dbać, by narzędzia GenAI były wykorzystywane w sposób odpowiedzialny i efektywny.

Zmaksymalizuj swoje inwestycje w bezpieczeństwo

Integracja GenAI z obecnymi narzędziami do ochrony może zwiększyć ich możliwości bez konieczności dokonywania dużych inwestycji. Takie podejście optymalizuje zwrot z dotychczasowych inwestycji w infrastrukturę i zapewnia, że GenAI uzupełnia oraz wzmacnia operacje bezpieczeństwa, co przekłada się na lepsze wyniki.

Na przykład wykorzystanie takich rozwiązań jak FortiAI może spowodować płynną integrację zaawansowanych możliwości AI z dotychczasową infrastrukturą Fortinet, zapewniając bardziej dogłębny wgląd i skuteczniejsze reagowanie na zagrożenia bez znacznych dodatkowych kosztów.
Dowiedz się więcej o integracji AI z Fortinet FortiAnalyzer.

4 października 2024 6:17 / 2757485-0-0-PL