Streszczenie

Orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego

Coraz więcej zespołów wytwarzających oprogramowanie korzysta obecnie z rozwiązań pozwalających na automatyzację większości czynności, które jeszcze kilka lat temu były wykonywane manualnie. Tego typu zmiany pozwalają na zwiększenie elastyczności procesów wytwarzania oprogramowania oraz umożliwiają szybsze wdrażanie zmian w oprogramowaniu i ich udostępnianiu użytkownikowi końcowemu. Niestety prowadzi to również do pewnych niedogodności. Największą z nich jest problem z zapewnieniem bezpieczeństwa tak zbudowanemu procesowi, w którym kod źródłowy aplikacji może się zmieniać nawet kilkanaście razy dziennie. Do dyspozycji zespołów bezpieczeństwa jest różnego rodzaju oprogramowanie, pozwalające na wykonywanie skanów podatności (w tym modelu realizacją manualnych testów bezpieczeństwa nie jest możliwa z uwagi na wolumen zmian).

Niestety automatyczne wykonywanie skanów podatności wiąże się ze zgłaszaniem (przez narzędzia) bardzo dużej liczby naruszeń, które muszą być odpowiednio przeanalizowane. Zarządzanie podatnościami bezpieczeństwa raportowanymi przez różnego rodzaju oprogramowanie skanujące jest skomplikowanym i czasochłonnym zajęciem. Konkretne błędy bezpieczeństwa mogą mieć różny wpływ na system teleinformatyczny w zależności od kontekstu, w jakim on działa. Co więcej, liczba błędów zgłaszanych przez konkretne rozwiązania może być bardzo duża (od kilkuset do kilku tysięcy), co zdecydowanie utrudnia analizę oraz określanie odpowiednich priorytetów dotyczących tego, które błędy należy usunąć w pierwszej kolejności.

Aby rozwiązać przedstawione powyżej problemy, w niniejszej rozprawie przedstawiono koncepcję rozwiązania *Mixeway*, które zostało wdrożone w infrastrukturze rzeczywistego operatora telekomunikacyjnego. Wspomniany system jest odpowiedzialny za orkiestrację pracy narzędzi bezpieczeństwa oraz umożliwia klasyfikację wykrytych podatności. Wykorzystany w *Mixeway* klasyfikator został przygotowany w procesie nauczania opartego o rzeczywiste dane zbierane przez 12 miesięcy z produkcyjnie działających aplikacji. Zebrane zagrożenia klasyfikowane są do jednej z dwóch kategorii: konieczne do poprawy w badanym kontekście (ang. Confirmed and Relevant Vulnerability - CRV) oraz nieistotne w badanym kontekście (ang. Detected but Not Relevant Vulnerability - DRNV). Wyniki uzyskane przez opracowany system *Mixeway* pozwalają potwierdzić skuteczność przedstawionego rozwiązania w kontekście automatycznej weryfikacji zagrożeń w procesie dostarczania oprogramowania.

Słowa kluczowe: bezpieczeństwo IT, CICD, devsecops, uczenie maszynowe