Oficjalnie, cyberprzestępczość stała się trzecią największą gospodarką świata. Co więcej, aktywność oszustów nie wykazuje oznak spowolnienia, ponieważ przeprowadzane są coraz bardziej wyrafinowane ataki. Nadążanie za cyberprzestępczością i wdrażanie odpowiedniego cyberbezpieczeństwa od samego początku procesu tworzenia oprogramowania jest teraz ważniejsze niż kiedykolwiek. Dlatego dzisiejszy artykuł odpowiada na pytanie, jak zapewnić bezpieczeństwo oprogramowania za pomocą DevSecOps.

>

Co to jest DevOps?

Zacznę od krótkiej odpowiedzi na pytanie: czym jest DevOps. DevOps to połączenie dwóch słów: rozwój i operacje. Co oznacza DevOps? Jest to po prostu szereg narzędzi, filozofii lub praktyk, które zapewniają dostarczenie produktu na czas. Osiąga się to poprzez połączenie pracy zespołów programistycznych i operacyjnych. Zespoły te są często łączone w jeden, co skutkuje jeszcze szybszym tworzeniem i wdrażaniem oprogramowania.

>

Czym zajmuje się DevOps?

W skrócie, DevOps pomaga szybciej tworzyć oprogramowanie. Jakie są jego największe zalety? Zwiększona wydajność i szybkość to rzeczywiście jedne z najczęściej wymienianych cech. Musimy jednak wspomnieć również o bezpieczeństwie. Stąd też często wyróżnia się DevSecOps. Cały pakiet szybkiego, wydajnego i bezpiecznego rozwoju i dostarczania służy jako główna zasada DevSecOps. Daje to przewagę konkurencyjną firmom i ich klientom w porównaniu do tradycyjnego rozwoju.

DevOps vs DevSecOps – jaka jest różnica?

Nie ma wyraźnego rozróżnienia między tym, czym jest DevOps, a czym DevSecOps. Niektórzy twierdzą, że kluczem jest większy nacisk kładziony na funkcje bezpieczeństwa w tym drugim. Inni twierdzą, że bezpieczeństwo powinno być oczywistą i wszechobecną cechą, o której nie trzeba wspominać w akronimie. Kto ma rację? W moim rozumieniu umieszczenie bezpieczeństwa w środku procesów

powinno być naturalne i oczywiste. Jeśli jednak niektórym trzeba przypomnieć o jego znaczeniu lub zapewnić klienta o związanych z nim funkcjach bezpieczeństwa, nie ma nic złego w używaniu tych terminów zamiennie. Najważniejszą częścią nie są szczegóły, takie jak nazwa. DecSecOps koncentruje się na zrozumieniu przez zespół znaczenia bezpieczeństwa i zgodności od samego początku. Zapewnia to ochronę integralności oprogramowania.

Co więcej, DevSecOps zapewnia płynną i bezproblemową integrację. Pozwala na wystarczającą kontrolę i widoczność organizacji, która może z łatwością przeprowadzać wnikliwe i złożone procesy bezpieczeństwa na każdym kroku.

>

Warto wspomnieć, że wiele środowisk może skorzystać na wdrożeniu DevSecOps. Niezależnie od tego, czy jest to środowisko lokalne, natywne w chmurze, czy hybrydowe, zastosowanie DevSecOps zapewnia maksymalną kontrolę nad całym cyklem życia oprogramowania.

>

8 obszarów DevSecOps poprawiających bezpieczeństwo

Co oznacza DevOps? DevOps usprawnia cykl życia oprogramowania. Oznacza to, że jest wdrażany w kluczowych obszarach rozwoju oprogramowania, ale także na każdym etapie cyklu życia. Te etapy to:

Planowanie

Przed rozpoczęciem prac kluczowe jest ich omówienie i zorganizowanie. Etap planowania obejmuje takie kroki, jak rozpoznanie pracy, która wymaga ukończenia, zorganizowanie jej przy użyciu priorytetyzacji oraz bezpieczne planowanie śledzenia i ukończenia od początku do końca.

>

Tworzenie

Zespół programistów pisze, projektuje i rozwija poprzez bezpieczne zarządzanie kodem i wszystkimi danymi.

Weryfikacja

Testowanie kodu i weryfikacja jego poprawności jest istotną częścią tworzenia oprogramowania. W końcu, jeśli jest wadliwy, cały projekt przestaje działać. Kontrole jakości i zautomatyzowane testowanie są również ważne dla zapewnienia bezpieczeństwa oprogramowania.

Pakowanie

Pakowanie oznacza tworzenie kontenerów i artefaktów oraz bezpieczne zarządzanie nimi.

Bezpieczeństwo

Testowanie oprogramowania koncentruje się w dużej mierze na bezpieczeństwie. Sprawdzanie luk w zabezpieczeniach odbywa się za pomocą testów dynamicznych i statycznych, a także skanowania zależności i testów fuzz.

Wdrożenie (Release)

Wydanie oprogramowania użytkownikom.

Monitorowanie

Faza monitorowania polega na śledzeniu wydajności wydanego oprogramowania i zmniejszaniu liczby incydentów oraz ich dotkliwości.

Zarządzanie (Konfiguracja)

Ta faza polega na zarządzaniu wadami i błędami w zabezpieczeniach, politykach i zgodności w całym oprogramowaniu.

SAILINGBYTE

Dlaczego używamy DevSecOps?

Istnieje kilka korzyści z wdrożenia DevSecOps w ramach tworzonego oprogramowania. Korzyści te można podzielić w zależności od trzech głównych obszarów: Rozwoju, Bezpieczeństwa i Operacji.

Korzyści dla programistów

- jedna aplikacja – korzystanie z takich narzędzi jak GitLab utrzymuje wszystkie funkcjonalności DevSecOps w jednym miejscu
- zwiększenie produktywności – pojedyncza aplikacja poprawia czas cyklu i zapobiega przełączaniu kontekstu
- automatyzacja w kluczowych obszarach – bogate w funkcje zautomatyzowane narzędzia pomagają usunąć niepotrzebną pracę.

Zalety związane z bezpieczeństwem

- wbudowane zabezpieczenia – testy buzz, API screening, DAST i inne są zintegrowane z oprogramowaniem, a nie dodawane
- odpowiednia zgodność – precyzyjne rozdzielenie obowiązków między zespołami nie jest już problemem dzięki DevSecOps; dostępne są szerokie rozwiązania dostosowywania, w tym dostosowane reguły zatwierdzania, które znacznie zmniejszają ryzyko
- automatyzacja – automatyczne skanowanie kodu w poszukiwaniu luk w zabezpieczeniach zapewnia szybki rozwój i dokładne wyniki testów.

Zalety operacyjne

- skalowalność – DevSecOps pomaga skalować firmy prawie bez przestojów

  .

- widoczność metryk – wszystkie dane dotyczące cyklu życia oprogramowania przechowywane w jednym miejscu (bez potrzeby dodatkowych integracji!)
- brak powiązań z dostawcą – narzędzie GitLab, którego używamy, nie jest ograniczone do jednego dostawcy chmury, więc nie ma blokady chmury.

Automatyzowane kontrole bezpieczeństwa i bezproblemowe wdrażanie oprogramowania z Sailing Byte

Każdy renomowany software house wie, że bezpieczeństwo jest kluczem do tworzenia oprogramowania. Sailing Byte nie tylko wdraża zabezpieczenia, ale także korzysta z najnowocześniejszych narzędzi i rozwiązań. Wszystko po to, aby zapewnić dwie kluczowe dla nas (i naszych klientów) cechy: łatwość i oszczędność czasu. Dzięki GitLab możemy nie tylko zapewnić najwyższy standard bezpieczeństwa, ale także jego automatyzację, co pozwala nam poświęcić więcej czasu na tworzenie najwyższej klasy oprogramowania. Zwiększona wydajność, bezpieczeństwo i skrócony czas kodowania? Raj dla wszystkich nowoczesnych programistów i ich klientów! Dodając do tego skalowalność i zgodność z przepisami, można uzyskać znaczne oszczędności i wygenerować zyski dla swojego przedsiębiorstwa. W końcu jeden mądry człowiek powiedział kiedyś, że czas to pieniądz. Bierzemy to sobie do serca i oszczędzamy go jak tylko możemy. Zaufaj nam, a my dostarczymy bezpieczny i bezbłędny produkt w najkrótszym możliwym czasie. Zarezerwuj telefon już dziś, aby omówić swój pomysł i jeszcze bardziej przyspieszyć proces.

>