



## Twórcy ABC DevSecOps:

Najlepsze szkolenie Andrzeja Dyjaka i Krzysztofa Korozeja

## DODAJ AUTOMATYZACJĘ BEZPIECZEŃSTA DO SWOJEGO ARSENAŁU

ABC DevSecOps™ to najlepsze w Polsce szkolenie DevSecOps dla inżynierów i deweloperów rozwijających kompetencje umożliwiające obronę aplikacji i infrastruktury IT przed poważnymi atakami – w całym procesie wytwarzania oprogramowania SDLC.

### Korzyści dla firmy i zespołu:

- Przesuniesz bezpieczeństwo "w lewo" (shift left). Dodasz narzędzia bezpieczeństwa (SAST, DAST, SCA) w odpowiednich miejscach procesu CI/CD i zaczniesz znajdować podatności wcześniej.
- Rozwiązesz problemy z automatyzacją bezpieczeństwa w procesie wytwórczym SDLC budując lub usprawniając procesy z nią związane.
- Zadbasz o bezpieczeństwo swoich projektów i będziesz o krok przed nadchodzącymi wymaganiami prawnymi takimi jak NIS2, DORA czy CRA.

### Dzięki formule online:

- Nie odrywamy Twojego zespołu od bieżących projektów.
- Cały materiał dostępny jest przez 365 dni od startu programu.
- Bogata agenda: Analiza Dynamiczna (DAST), Fuzzing, Analiza Statyczna (SAST), Analiza Składników Oprogramowania (SCA), Supply-chain, SBOM, Vulnerability Management, i wiele innych!

## Dołącz do ABC DevSecOps

Szczegółowy program: [www.abcdevsecops.pl](http://www.abcdevsecops.pl)

### Masz dodatkowe pytania?

Skontaktuj się z nami, odpowiemy szybko!



Rafał Goliszewski  
Koordynator Kursu  
rafal@bezpiecznykod.pl



### Andrzej Dyjak

Prowadzi firmę doradczo-szkoleniową **Bezpieczny Kod**. W przeszłości pomógł poprawić bezpieczeństwo aplikacji firm takich jak **Apple, Google, Oracle, Mozilla** czy **Real Networks**.

W ostatnich latach przeszkolił **setki** specjalistów IT (QA, Dev, Ops) z tematów takich jak Testowanie Bezpieczeństwa, Modelowanie Zagrożeń, DevSecOps oraz Secure By Design.

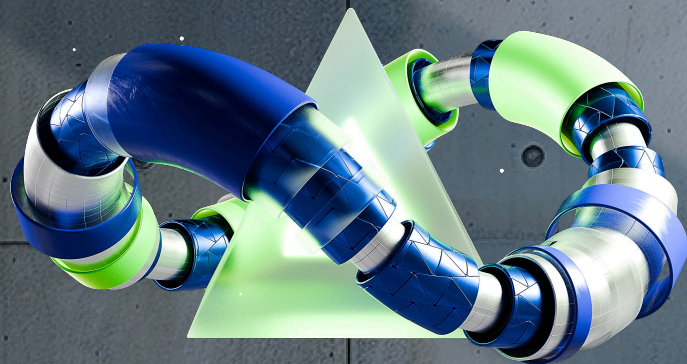


### Krzysztof Korozej

Senior Product Security Engineer w **Tidio** (**12m+ użytkowników**), w którym **zbudował procesy wokół DevSecOps**, a następnie stworzył zespół zarządzający nimi.

Ex-QA z doświadczeniem, które pomaga zrozumieć mu działanie zespołów wytwórczych i proces SDLC.

**Prelegent** na największych konferencjach dotyczących IT (**The Hack Summit, 4Developers**).



**Start: 28 kwietnia**

**Zakończenie: 1 czerwca**

Szkolenia Bezpiecznego Kodu ukończyło ponad 1500 inżynierów i inżynierów z firm takich jak Orange, BNP Paribas, XTB, Grupa Pracuj, Autopay i wielu innych.

### Cena uczestnictwa

**1790 zł + 23% VAT / od osoby**  
**2201,70 zł brutto**

3-5 osób -10%

6-30 osób -15%

30+ osób -20%

Możliwe finansowanie:

– 2 raty 0%.

Moduł 0	Tematy	Rezultaty	Projekty i Bonusy
<b>Fundamenty DevSecOps aka „Bootloader”</b>	<p>DevSecOps czyli co?</p> <p>DevOps, Potok CI/CD.</p> <p>Fundamentalne pryncypia DevSecOps.</p>	<ul style="list-style-type: none"> <li>Zbudujesz lub zrewidujesz koncepcję pipeline CI/CD (dla swojej firmy).</li> <li>Poznasz wzorcowy model pipeline CI/CD ze wszystkimi fundamentalnymi praktykami DevSecOps.</li> </ul>	<ul style="list-style-type: none"> <li>Zbudowanie diagramu architektury referencyjnej dla własnego potoku CI/CD.</li> <li>Stworzenie 'Gap Analysis' pomiędzy stanem faktycznym, a architekturą referencyjną.</li> <li><b>BONUS:</b> Mapa architektury referencyjnej DevSecOps użytej w kursie.</li> </ul>
<b>Moduł 1</b>	<b>Tematy</b>	<b>Rezultaty</b>	<b>Projekty i Bonusy</b>
<b>Analiza Dynamiczna (DAST)</b>	<p>Podstawowy skan DAST (1st gen, ZAP) na web aplikację.</p> <p>Skanowanie Pasywne vs Aktywne.</p> <p>Skanowanie AuthN vs non-AuthN wraz z omówieniem problemów wynikających z różnych rodzajów uwierzytelnień.</p> <p>Fuzzing i dodatkowe payloady.</p> <p>Skan DAST (2nd gen, nuclei) i podejście Test-Driven Security.</p> <p>Wbudowanie podstawowego skanu DAST w nasz archetypowy potok CI/CD.</p>	<ul style="list-style-type: none"> <li>Przeprowadzisz skan dynamiczny web aplikacji (DAST, ZAP).</li> <li>Wbudujesz skanowanie w potok CI.</li> <li>Poznasz narzędzie DAST 2-giej generacji pozwalające na Test-Driven Security.</li> <li>Poprawisz templatki / POC z wykorzystaniem <b>AI</b>.</li> </ul>	<ul style="list-style-type: none"> <li>Wbudowanie skanów DAST w potok CI/CD.</li> <li>Integracja wyników skanów z centralnym dashboardem.</li> <li>Napisanie templatki nuclei.</li> <li>Wykorzystanie GPT do napisania nowej templatki.</li> </ul>
<b>Moduł 2</b>	<b>Tematy</b>	<b>Rezultaty</b>	<b>Projekty i Bonusy</b>
<b>Analiza składu i łańcuch dostaw (SCA, supply-chain)</b>	<p>Problem podatnych bibliotek i problem niekompatybilnych licencji.</p> <p>SBOM, bez integracji z Dependency Trackiem.</p> <p>Skanowanie Lokalne vs Globalne.</p> <p>Działania PROAKTYWNE i działania RETROAKTYWNE. Różnice.</p> <p>Problem złośliwych bibliotek i ataki na łańcuch dostawczy.</p> <p>Ocena dojrzałości zależności/bibliotek projektów. Różnice pomiędzy OpenSSF, Packj, Guarddog.</p> <p>Czym jest Provenance (via SLSA).</p>	<ul style="list-style-type: none"> <li>Wdrożysz narzędzie klasy SCA na różnych etapach swojego procesu SDLC (lokalnie oraz pipeline CI/CD).</li> <li>Wygenerujesz SBOM dla swojego projektu.</li> <li>Ocenisz dojrzałość bibliotek dla swoich projektów (via OpenSSF).</li> <li>Zbudujesz pierwszą linię obrony przed złośliwymi zależnościami.</li> </ul>	<ul style="list-style-type: none"> <li>Wbudowanie skanów SCA w potok CI/CD.</li> <li>Integracja wyników skanów z centralnym dashboardem.</li> <li><b>BONUS:</b> Efekt zawirusowania licencji - sprawdź bezpieczeństwo użytych licencji oraz stwórz dla nich black listę i white listę.</li> </ul>
<b>Moduł 3</b>	<b>Tematy</b>	<b>Rezultaty</b>	<b>Projekty i Bonusy</b>
<b>Analiza statyczna: Podstawy (SAST 101)</b>	<p>Sekrety w kodzie. Metody detekcji sekretów.</p> <p>Problemy z False Positives.</p> <p>Skany Lokalne vs Globalne.</p> <p>Proaktywność vs Retroaktywność.</p> <p>Sekrety jako problem kodu i infrastruktury - skanowanie obrazów Docker, szukanie sekretów w logach</p> <p>Rotacja. Co zrobić gdy trafisz na sekret?</p> <p>SAST (styczna analiza kodu) jako podstawa podejścia "Secure by Default".</p>	<ul style="list-style-type: none"> <li>Zapobiegiesz wprowadzaniu nowych sekretów do kodu źródłowego.</li> <li>Zintegrujesz szukanie sekretów w potoku CI.</li> <li>Wykorzystasz sekrety jako IOC.</li> <li>Stworzysz własny wzorzec z <b>AI</b></li> </ul>	<ul style="list-style-type: none"> <li>Wbudowanie skanowania sekretów w potok CI/CD.</li> <li>Konfiguracja Gita w celu działania proaktywnego.</li> <li>Integracja wyników skanów z centralnym dashboardem.</li> <li><b>BONUS:</b> Sekrety jako IOC (Indicator of Compromise).</li> </ul>
<b>Moduł 4</b>	<b>Tematy</b>	<b>Rezultaty</b>	<b>Projekty i Bonusy</b>
<b>Analiza statyczna: Zaawansowane (SAST 102)</b>	<p>Podstawowy skan SAST 1st gen na web aplikację. Podstawowy skan SAST 2nd gen i wprowadzenie do Semgrep.</p> <p>Przegląd dostępnych narzędzi - 1st gen i 2nd gen. Skany Lokalne vs Globalne.</p> <p>Pisanie własnych reguł w wersji podstawowej plus zaawansowane techniki doskonalenia reguł. Strategia wdrażania do potoku CI/CD.</p> <p>Skanowanie plików Infrastructure-as-Code i podejście Compliance-as-Code.</p> <p>Automatyczny skan podatności klasycznej infrastruktury.</p>	<ul style="list-style-type: none"> <li>Wdrożysz SAST zarówno lokalnie jak i globalnie.</li> <li>Napiszesz własną regułę, zarówno podstawową jak i zaawansowaną (SAST, Semgrep).</li> <li>Stworzysz własne reguły SAST z <b>AI</b></li> <li>Uruchomisz skan na pliki konfiguracyjne.</li> <li>Wykonasz podstawowy skan podatności infrastruktury.</li> </ul>	<ul style="list-style-type: none"> <li>Wbudowanie skanów SAST w potok CI/CD.</li> <li>Napisanie i udoskonalenie własnej reguły.</li> <li>Wbudowanie Compliance-as-Code w potok CI/CD.</li> <li>Wbudowanie automatycznych skanów podatności w potok CI/CD.</li> <li>Integracja wyników skanów z centralnym dashboardem.</li> </ul>
<b>Moduł 5</b>	<b>Tematy</b>	<b>Rezultaty</b>	<b>Projekty i Bonusy</b>
<b>Vulnerability Management</b>	<p>Czym jest VM i czym się różni w procesie DevSecOps od zwykłego klasycznego podejścia (skany podatności).</p> <p>SLA dla wyprowadzania podatności.</p> <p>Budowanie własnego Knowledge Base (KB).</p> <p>Ocena krytyczności vs ocena ryzyka.</p>	<ul style="list-style-type: none"> <li>Przełożysz umiejętności z poprzednich tygodni na efekt biznesowy dla firmy.</li> <li>Podjędziesz decyzje biznesowe związane z wbudowywaniem bezpieczeństwa w potok CI/CD.</li> </ul>	<ul style="list-style-type: none"> <li><b>BONUS:</b> Finalny efekt: Gotowy pipeline CI/CD, który wykonuje wszystkie skany omawiane w kursie.</li> </ul>

Masz dodatkowe pytania?

Skontaktuj się z nami, odpowiemy szybko!



**Rafał Goliszewski**  
Koordynator Kursu  
rafal@bezpiecznykod.pl