Bezpieczny Kod

Katalog ofertowy na szkolenia i usługi doradcze

Wrzesień 2024

Spis treści

1. O naszej firmie

Bezpieczny Kod to lider na polskim rynku w obszarze bezpieczeństwa aplikacji i procesu wytwórczego SDLC. Łączymy wieloletnie doświadczenie z innowacyjnym podejściem, oferując ekspercką wiedzę zarówno w ofensywnych, jak i defensywnych aspektach.

Oferujemy usługi audytorskie, doradcze i szkoleniowe w zakresie bezpieczeństwa procesu wytwórczego SDLC, automatyzacji bezpieczeństwa w potokach CI/CD, modelowania zagrożeń i analizy ryzyka, testowania i weryfikacji bezpieczeństwa oraz całościowego zarządzania cyberbezpieczeństwem.

Mieliśmy zaszczyt doradzać lub szkolić członków zespołów deweloperskich u klientów takich jak:

BNP PARIBAS, orange, COMARCH, BIK, PayPo

URZĄD OCHRONY DANYCH OSOBOWYCH, DZP, UNIWERSYTET ŚLĄSKI W KATOWICACH, Urząd Ochrony Konkurencji i Konsumentów, MAIN

VULCAN, nowa era, Autopay, 7N, THE SOFTWARE HOUSE

To z czego jesteśmy dumni w liczbach:

- **1500+** uczestników szkoleń,
- **100+** zrealizowanych projektów,
- **30+** lat doświadczenia (łącznie).

Oddajemy społeczności

Z pasją dzielimy się naszym doświadczeniem, inspirując i edukując społeczność IT. Oprócz newslettera (obecnie **ponad 3500 odbiorców**), naszą wiedzą dzielimy się również na inne sposoby.

Jednym z nich jest nasz podcast **“Bezpieczny Kod Podcast”,** który żyje na styku cyberbezpieczeństwa i rozwoju oprogramowania.

W audycjach przybliżamy kluczowe aspekty cyberbezpieczeństwa istotne dla nowoczesnych zespołów deweloperskich. Czasem we własnym gronie, czasem z gośćmi – zawsze merytorycznie.

Znajdziesz nas na **YouTube** ↗, **Spotify** ↗, **Apple Podcasts** ↗ i każdej innej dużej platformie.

Dodatkowo nasz zespół wiodący nieustannie udziela się na konferencjach poświęconych cyberbezpieczeństwu, nierzadko zasiadając w **radach programowych** i opiekując się przebiegiem samych konferencji.

2. Współpraca

1. Poznajemy się podczas **darmowej konsultacji.** Omawiamy Twój problem, identyfikujemy potrzeby i określamy wstępne założenia projektu. W ciągu 5 dni roboczych otrzymujesz od nas dopasowaną ofertę, uwzględniającą Twoje unikalne wyzwania.

2. Przechodzimy przez niezbędne procesy formalne (NDA, wycena, harmonogram). Wspólnie definiujemy kluczowe rezultaty projektu – mogą to być konkretne deliverables (np. raporty z audytów, plany naprawcze) lub mierzalne KPI, w zależności od charakteru usługi. Opracowujemy **szczegółowy plan projektu,** ustalamy sposoby komunikacji i wyznaczamy punkty kontaktowe.

3. **Realizujemy projekt,** systematycznie dostarczając uzgodnione rezultaty. Prowadzimy regularne check-iny, weryfikując postępy i dostosowując działania do Twoich potrzeb. Po osiągnięciu celów, organizujemy spotkanie podsumowujące, prezentujemy końcowe deliverables, zbieramy feedback i omawiamy możliwości dalszej współpracy.

3. Szkolenia

Wdrożenie odpowiednich praktyk na etapie procesu wytwórczego SDLC pozwala rozwiązywać problemy bezpieczeństwa, zanim kod trafi na produkcję. Nasze programy szkoleniowe pomogą Twojemu zespołowi nabyć kluczowe umiejętności do skutecznej realizacji tego celu.

Na to możesz liczyć:

- **Doświadczenie zdobyte w boju.** To czego uczymy jest efektem wielu lat praktyki. Przez ten czas zdobyliśmy bogate doświadczenie zarówno od strony ofensywnej jak i defensywnej.
- **Programy oparte o standardy.** Nasze szkolenia opieramy o globalne standardy, dlatego podczas audytu mogą one pełnić rolę dowodu due diligence w kwestii edukacji zespołów.
- **Praktyczne podejście do nauki.** Wierzymy, że umiejętności buduje się poprzez działanie, dlatego w każdym programie kładziemy nacisk na pracę praktyczną z teorią w tle.

Pomożemy Twojemu zespołowi nabyć kluczowe umiejętności w cyberbezpieczeństwie.

3.1. Automatyzacja Bezpieczeństwa w CI/CD: DevSecOps (ABCD)

Automatyzacja bezpieczeństwa w potoku CI/CD stanowi fundament DevSecOps. Jej kluczowa rola polega na skracaniu pętli zwrotnej, co znacząco redukuje koszty bezpieczeństwa w całym cyklu wytwórczym SDLC.

To szkolenie wyposaży Twój zespół w umiejętności efektywnego wbudowania do potoku CI/CD kluczowych praktyk, takich jak Analiza Dynamiczna (DAST), Analiza Statyczna (SAST) czy Analiza Składu Oprogramowania (SCA). Dzięki temu uczestnicy będą w stanie zautomatyzować procesy testowania bezpieczeństwa i znacząco przyspieszyć wykrywanie oraz naprawę podatności.

Szczegóły organizacyjne:

- Idealnymi **odbiorcami** szkolenia są Programiści, Administratorzy, DevOps, Testerzy i Inżynierzy QA oraz Inżynierzy Bezpieczeństwa.
- Szkolenie jest w formie **interaktywnego warsztatu** 70:30 – większość czasu (70%) spędzamy wykonując praktyczne ćwiczenia, a pozostałą część (30%) poznając teorię.
- Czas trwania szkolenia w formie stacjonarnej to **2 pełne dni** szkoleniowe.
- Efektywne **przerabianie programu wymaga** posiadania komputera, środowiska wirtualnego (VM), oraz Dockera. Przed szkoleniem dostarczamy instrukcję co należy zainstalować.

Program „Automatyzacja Bezpieczeństwa w CI/CD: DevSecOps” oferujemy również jako **kohortowy kurs online**. Edycja trwa 5+1 tygodni z cotygodniowymi spotkaniami online i wspólnym przerabianiem materiału. Dodatkowy tydzień przeznaczony jest na uzupełnienie zaległości i oddanie prac domowych.

Dowiedz się więcej ↗

3.1.1. Agenda skrócona

- **Fundamenty DevSecOps.** Uczestnicy poznają koncepcję DevSecOps, jej związek z DevOps oraz rolę w tworzeniu bezpiecznego oprogramowania. Zgłębią wpływ DevSecOps na potok CI/CD i kluczowe zasady skutecznego wdrażania tej metodologii.

- **Analiza Dynamiczna (DAST).** Uczestnicy poznają podstawy i zaawansowane techniki DAST, używając narzędzi pierwszej (ZAP) i drugiej (Nuclei) generacji. Zgłębią różnice między skanowaniem pasywnym a aktywnym, z uwierzytelnieniem i bez. Zapoznają się z technikami fuzzingu i koncepcją Test-Driven Security. Nauczą się integrować DAST z potokiem CI/CD.

- **Analiza Składu (SCA) i łańcuch dostaw.** Uczestnicy zgłębią problematykę podatnych bibliotek, niekompatybilnych licencji oraz koncepcję SBOM. Poznają różnice między skanowaniem lokalnym a globalnym w SCA oraz działania proaktywne i retroaktywne. Zapoznają się z zagrożeniami łańcucha dostaw, oceną dojrzałości zależności oraz narzędziami jak OpenSSF i Guarddog. Zgłębią koncepcję Provenance w kontekście standardu SLSA.

- **Analiza Statyczna (SAST): Podstawy.** Uczestnicy poznają metody detekcji sekretów w kodzie, obrazach Docker i logach, ucząc się radzić z fałszywymi pozytywnymi wynikami. Zgłębią różnice między skanowaniem lokalnym a globalnym oraz podejściem proaktywnym i retroaktywnym. Zapoznają się z procedurami rotacji sekretów. Moduł wprowadzi również podstawy Statycznej Analizy Kodu (SAST) jako fundament podejścia „Secure by Default”.

- **Analiza Statyczna (SAST): Zaawansowane.** Uczestnicy poznają techniki SAST pierwszej i drugiej generacji, w tym narzędzie Semgrep. Zgłębią różnice między skanami lokalnymi a globalnymi oraz strategie wdrażania SAST w CI. Nauczą się pisać własne reguły SAST i skanować Infrastructure-as-Code. Poznają podejście Compliance-as-Code i metody automatycznego skanowania klasycznej infrastruktury.

- **Zarządzanie podatnościami.** Uczestnicy zgłębią zarządzanie podatnościami (VM) w kontekście DevSecOps, poznając różnice wobec tradycyjnego podejścia. Nauczą się ustalać SLA dla eliminowania podatności i budować własną bazę wiedzy. Zrozumieją

różnice między oceną krytyczności a oceną ryzyka podatności, co pomoże w priorytetyzacji działań naprawczych.

Szczegółowa agenda programu ABCD znajduje się w załączniku.

3.2. Ofensywne Testowanie Web Aplikacji (OTWA)

Testowanie bezpieczeństwa stanowi fundament skutecznej ochrony aplikacji i systemów IT. Wdrożone w odpowiednich punktach procesu wytwórczego SDLC potrafi redukować koszty późniejszych poprawek.

To szkolenie wyposaży Twój zespół deweloperski w umiejętność identyfikacji krytycznych podatności. Program opiera się na uznanych standardach, takich jak OWASP Top 10, ASVS czy WSTG. Dzięki temu uczestnicy nie tylko uczą się rozpoznawać zagrożenia, ale także zdobywają praktyczną wiedzę, jak im skutecznie przeciwdziałać i podnosić poziom bezpieczeństwa w swoich projektach.

Szczegóły organizacyjne:

- Idealnymi **odbiorcami** szkolenia są Programiści, Testerzy i Inżynierzy QA, Administratorzy, DevOps, oraz Inżynierzy Bezpieczeństwa.
- Szkolenie jest w formie **interaktywnego warsztatu** 80:20 – większość czasu (80%) spędzamy wykonując praktyczne ćwiczenia, a pozostałą część (20%) poznając teorię.
- Czas trwania szkolenia w formie stacjonarnej to **2 pełne dni** szkoleniowe.
- Efektywne **przerabianie programu wymaga** posiadania komputera, środowiska wirtualnego (VM), oraz Dockera. Przed szkoleniem dostarczamy instrukcję co należy zainstalować.

Program „Ofensywne Testowanie Web Aplikacji” oferujemy również jako **kohortowy kurs online**. Edycja trwa 5+1 tygodni z cotygodniowymi spotkaniami online i wspólnym przerabianiem materiału. Dodatkowy tydzień przeznaczony jest na uzupełnienie zaległości i oddanie prac domowych.

Dowiedz się więcej ↗

3.2.1. Agenda skrócona

- **Fundamenty cyberbezpieczeństwa.** Uczestnicy poznają fundamenty działania sieci Web, w tym protokół HTTP, strukturę DOM oraz mechanizmy bezpieczeństwa jak SOP i CORS. Zgłębią Triadę CIA (Poufność, Integralność, Dostępność) jako podstawę bezpieczeństwa informacji. Zrozumieją różnice między CorpSec, NetSec i AppSec w kontekście całościowego podejścia do cyberbezpieczeństwa. Poznają różne metody oceny bezpieczeństwa aplikacji i systemów IT, w tym specyfikę testowania Black-box, Gray-box oraz White-box.

- **Rekonesans i enumeracja.** Uczestnicy nauczą się odkrywać stos technologiczny web aplikacji i skanować je pod kątem dostępnych zasobów. Poznają techniki automatycznego skanowania podatności serwera web oraz weryfikacji bezpieczeństwa certyfikatów SSL/TLS. Zgłębią metody aktywnego podsłuchu ruchu sieciowego i wykrywania Web Application Firewalls (WAF).

- **Podatności w AuthZ i wstrzyknięcia kodu.** Uczestnicy nauczą się wykorzystywać podatność IDOR do uzyskania nieautoryzowanego dostępu do danych. Poznają techniki przeprowadzania ataków XSS, symulując realne scenariusze wykradania ciasteczek użytkowników. Zgłębią metody automatycznego skanowania podatności web aplikacji z użyciem niestandardowych payloadów (Fuzzing).

- **Błędna logika, konfiguracja & podatne biblioteki.** Uczestnicy poznają proces Modelowania Zagrożeń i pryncypia bezpiecznej architektury. Nauczą się wykrywać podatności w logice biznesowej, skupiając się na mechanizmach uwierzytelniania. Zgłębią analizę nagłówków bezpieczeństwa, w tym ocenę poprawności polityk HSTS i CSP. Poznają techniki automatycznego skanowania podatności bibliotek oraz obrazów Dockerowych.

- **Podatności w AuthN, integralność & automatyzacja ataków.** Uczestnicy nauczą się przeprowadzać ataki siłowe na mechanizmy uwierzytelniania web aplikacji i usług (np. OpenSSH). Poznają metody automatyzacji procesu wykrywania podatności poprzez Analizę Dynamiczną (DAST). Zgłębią techniki atakowania łańcucha dostawczego na przykładzie front-end oraz zrozumieją rolę mechanizmu Subresource Integrity (SRI) w ochronie przed takimi atakami.

- **Raportowanie.** Uczestnicy nauczą się oceniać krytyczność wykrytych problemów bezpieczeństwa, wykorzystując systemy CVE i CVSS. Poznają metody identyfikacji znanych podatności oraz techniki klasyfikacji nowo odkrytych zagrożeń z użyciem VRT. Zgłębią charakterystykę efektywnego raportu z testów bezpieczeństwa. Na zakończenie, zdobędą wiedzę o możliwych ścieżkach dalszego rozwoju w dziedzinie bezpieczeństwa aplikacji webowych.

Szczegółowa agenda programu OTWA znajduje się w załączniku.

3.3. Praktyczne Modelowanie Zagrożeń (PMZ)

Modelowanie zagrożeń to kluczowy element proaktywnego podejścia do cyberbezpieczeństwa. Przewidywanie i rozwiązywanie problemów bezpieczeństwa na etapie projektowania znacząco redukuje koszty związane z utrzymaniem systemu IT oraz minimalizuje ryzyko późniejszych incydentów.

To szkolenie wyposaży Twój zespół w umiejętności efektywnego i praktycznego modelowania zagrożeń. Uczestnicy nauczą się identyfikować potencjalne problemy bezpieczeństwa już na wczesnych etapach rozwoju projektu, co pozwoli im unikać kosztownych poprawek w fazie implementacji i testowania. Po tym programie Twój zespół będzie w stanie tworzyć bezpieczniejsze systemy.

Szczegóły organizacyjne:

- Idealnymi **odbiorcami** szkolenia są Programiści, Architekci, Projektanci, Testerzy i Inżynierzy QA, Administratorzy, DevOps oraz Inżynierzy Bezpieczeństwa.
- Szkolenie jest w formie **interaktywnego warsztatu** 70:30 – większość czasu (70%) spędzamy wykonując praktyczne ćwiczenia, a pozostałą część (30%) poznając teorię.
- Czas trwania szkolenia w formie stacjonarnej to **1 pełny dzień** szkoleniowy.
- Efektywne **przerabianie programu wymaga** dostępu do tablicy. Żaden sprzęt elektroniczny **nie jest** wymagany.

Program „Praktyczne Modelowanie Zagrożeń” oferujemy również jako szkolenia otwarte w formie stacjonarnej oraz online. Najbliższe terminy zostaną opublikowane na początku 2024Q4.

3.3.1. Agenda skrócona

- **Bezpieczny proces wytwórczy SDLC.** Uczestnicy poznają fundamenty zarządzania bezpieczeństwem aplikacji, w tym kluczowe aspekty zarządzania podatnościami. Nauczą się, jak efektywnie budować wymagania bezpieczeństwa dla systemów IT.

Zgłębią różnorodne metody oceny bezpieczeństwa systemów informatycznych, tworząc solidną podstawę do praktycznego modelowania zagrożeń.

- **Modelowanie Zagrożeń: Teoria.** Uczestnicy zgłębią różne poziomy i podejścia do modelowania zagrożeń, w tym metodę Attack Trees, model STRIDE wraz z jego rozszerzeniem TRIM, oraz techniki takie jak diagramy przepływu danych (DFD), DREAD i matryce ryzyka (Risk Matrix). Poznają zasady Agile Threat Modeling, dostosowując techniki do dynamicznego środowiska rozwoju oprogramowania. Przeanalizują dostępne narzędzia wspierające proces modelowania zagrożeń, takie jak: TMT, Deciduous, Elevation of Privilege & Privacy czy Cornucopia.
- **Modelowanie Zagrożeń: Praktyka.** Uczestnicy przeprowadzą praktyczne ćwiczenia modelowania zagrożeń na trzech kluczowych poziomach: infrastruktury, aplikacji oraz konkretnej funkcjonalności. Wykorzystają szereg narzędzi i technik poznanych wcześniej, w tym diagramy przepływu danych (DFD), modele STRIDE i TRIM, metodykę DREAD, matryce ryzyka oraz drzewa ataków (Attack Trees). Te praktyczne mini-sesje pozwolą uczestnikom zintegrować zdobytą wiedzę i zastosować ją w realistycznych scenariuszach, rozwijając umiejętność kompleksowej analizy bezpieczeństwa systemów IT.

Szczegółowa agenda znajduje się w załączniku.

3.4. Opinie o naszych programach

Szkolenie było dla mnie maksymalnie merytoryczne, praktyczne i ciekawe. Dostałem ogrom skomplikowanej wiedzy przekazanej w sposób prosty i przejrzysty.

— Łukasz Zajączkowski, QA Engineer

Ze względu na dynamiczny charakter dziedziny bezpieczeństwa aplikacji, szkolenie powinno uwzględniać najnowsze zagrożenia, techniki ataków i narzędzia obronne. Szkolenie oparte jest na aktualnych trendach i praktykach. Super praktyczne ćwiczenia.

— Maciej Bartkowski, Head of Security Department

Fantastyczne szkolenie! Wszystkie koncepty omówione bez zbędnego rozwlekania, wszystko w punkt!

— Paweł Tutka, DevOps Engineer

Wiedza wyniesiona stała się zalążkiem do e-booka o bezpieczeństwie, który napisałem razem z moją firmą. Jeżeli chcesz pisać bezpieczne aplikacje, OTWA jest dla Ciebie!

— Rafał Hofman, Software Engineer

Jestem pod wielkim wrażeniem umiejętności Andrzeja i polecam wszystkim uczestnictwo w organizowanych przez niego szkoleniach. To naprawdę duża dawka solidnej wiedzy z zakresu cyberbezpieczeństwa.

— Tomasz Kuciński, Główny Administrator Systemu

Udział w kursie nie tylko dostarczył mi wiedzy na temat cybersecurity, którą będę wykorzystywać w codziennej pracy, ale także dużo zabawy przy atakowaniu aplikacji Juice Shop!

— Karolina Dyrda, QA Specialist

Dowiemy się nie tylko jak jak testować i pisać bezpieczne oprogramowanie ale co równie ważne dlaczego powinniśmy to robić. Dzięki niemu usystematyzowałem wiedzę, usprawniłem używane procesy DevSecOps i wprowadziłem nowe.

— Lucjan, DevOps Engineer

Materiał szkoleniowy był bardzo dobrze przygotowany i zawierał mnóstwo praktycznych informacji, które z pewnością będą przydatne w codziennej pracy związanej z testowaniem aplikacji webowych. Na plus należy także zaliczyć różnorodność tematów poruszanych podczas szkolenia, co pozwoliło na zrozumienie zagadnień związanych z ofensywnym testowaniem od strony technicznej, ale także z punktu widzenia procesów i strategii.

— Adrian Maryniewski, QA Engineer

W programie zawarte są kluczowe zagadnienia, standardy i wytyczne dotyczące testowania bezpieczeństwa, techniki wykrywania podatności, a także wymagania dotyczące ich raportowania. Polecam wszystkim, którzy chcą specjalizować się w tym obszarze cyberbezpieczeństwa!

— Marek Kost, Senior Security Professional (CISM, CISA, CRISC)

4. Doradztwo i audyty

Nasze usługi doradcze pomagają w systematycznym eliminowaniu podatności, zapobieganiu nowym zagrożeniom oraz obniżeniu długoterminowych kosztów związanych z cyberbezpieczeństwem. Z nami osiągniesz cele biznesowe, jednocześnie wzmacniając bezpieczeństwo Twojej organizacji.

Na to możesz liczyć:

- **Działanie w Twoim interesie.** Cyberbezpieczeństwo jest zarówno szerokie jak i głębokie. Naszym zadaniem jako zaufanego doradcy jest pomóc Ci znaleźć drogę, wypracować plan i dotrzeć do celu.
- **Zrozumienie kontekstu biznesowego.** Wiemy, że cyberbezpieczeństwo jest kosztem. Pomożemy Ci zmaksymalizować zwrot z inwestycji w cyberbezpieczeństwo i zminimalizować ryzyko związane z IT.
- **Strategiczne podejście do rozwiązań.** Wspólnie zadbamy o bezpieczeństwo na każdym etapie procesu SDLC: Od fazy projektowania, przez fazy implementacji i weryfikacji aż do fazy wydania i utrzymania.

Eliminuj podatności, zapobiegaj zagrożeniom i obniżaj koszty cyberbezpieczeństwa.

W przeszłości znaleźliśmy podatności w oprogramowaniu największych dostawców:

Google ORACLE Adobe moz://a

4.1. Usługi główne

4.1.1. Doradztwo strategiczne

Doradztwo strategiczne umożliwia osiągnięcie długoterminowego bezpieczeństwa i efektywności IT w organizacji. Pomaga wyznaczyć kierunek i zoptymalizować procesy cyberbezpieczeństwa.

Oferujemy doradztwo eksperckie w obszarach: Strategii Secure SDLC, Transformacji DevSecOps. Dla wybranych klientów możemy pełnić rolę zaufanego doradcy w formule Virtual CISO / Fractional CISO.

4.1.2. Audyty bezpieczeństwa

Audyt to kluczowy pierwszy krok w poprawie bezpieczeństwa. Pozwala ocenić obecność i skuteczność kontroli bezpieczeństwa.

Oferujemy specjalistyczne audyty w obszarach: Dojrzałości DevSecOps, platform deweloperskich, architektury rozwiązań, bezpiecznej implementacji AI, środowisk chmurowych czy kodu źródłowego.

4.2. Usługi uzupełniające

4.2.1. Analiza i modelowanie

Analiza i modelowanie są szczególnie ważne w proaktywnym podejściu do cyberbezpieczeństwa. Pozwalają zidentyfikować potencjalne zagrożenia i ocenić ryzyko przed wystąpieniem incydentów.

Oferujemy specjalistyczne usługi w obszarach: Modelowania Zagrożeń dla konkretnych rozwiązań oraz Analizy Profilu Ryzyka dla pojedynczych systemów lub całej organizacji.

4.2.2. Testy bezpieczeństwa

Testy bezpieczeństwa to kluczowy element w identyfikacji podatności w systemach IT. Mogą być częścią większego audytu lub stanowić osobną inicjatywę. Pomagają wykryć podatności w implementacji, łańcuchy ataków i sposoby eskalacji.

Oferujemy specjalistyczne testy w obszarach: bezpieczeństwa web aplikacji i API, bezpieczeństwa aplikacji mobilnych oraz testy penetracyjne systemów IT.

4.2.3. Wsparcie technologiczne

Wsparcie technologiczne pozwala skutecznie wdrażać i utrzymywać rozwiązania bezpieczeństwa. Pomaga również w optymalizacji procesów i efektywnym wykorzystaniu narzędzi.

Oferujemy specjalistyczne wsparcie w obszarach: implementacji narzędzi (np. SAST czy DAST), optymalizacji procesów bezpieczeństwa oraz mentoringu technologicznego dla zespołów IT.

4.2.4. Zgodność i standardy

Ocena zgodności stanowi fundament w zapewnieniu, że organizacja spełnia wymogi prawne i branżowe w zakresie cyberbezpieczeństwa. Umożliwia identyfikację luk i przygotowanie do audytów.

Oferujemy specjalistyczne usługi w obszarach: oceny zgodności z regulacjami (np. NIS2, DORA, CRA, PCI DSS) oraz wsparcia w uzyskaniu certyfikacji (np. ISO 27001, SOC2).

4.2.5. Szkolenia dla firm

Wdrożenie odpowiednich praktyk na etapie procesu wytwórczego SDLC pozwala rozwiązywać problemy bezpieczeństwa, zanim kod trafi na produkcję. Nasze programy szkoleniowe pomogą Twojemu zespołowi nabyć kluczowe umiejętności do skutecznej realizacji tego celu.

Szczegóły w sekcji szkolenia.

5. Załączniki

Załącznik A: Szczegółowa agenda programu “Automatyzacja Bezpieczeństwa w Potoku CI/CD: DevSecOps”

1. Fundamenty DevSecOps
1.1. Uczestnicy dowiedzą się, czym jest DevSecOps i jaką rolę pełni w tworzeniu bezpiecznego oprogramowania.
1.2. Poznają związek między DevSecOps a DevOps.
1.3. Zgłębią koncepcję potoku CI/CD i zrozumieją, jak DevSecOps wpływa na ten proces.
1.4. Zapoznają się z głównymi zasadami DevSecOps, które są kluczowe dla skutecznego wdrażania.
2. Analiza Dynamiczna (DAST)
2.1. Uczestnicy poznają podstawy skanowania DAST, wykorzystując narzędzia pierwszej generacji, takie jak ZAP, do analizy aplikacji webowych.
2.2. Zgłębią różnice pomiędzy skanowaniem pasywnym a aktywnym.
2.3. Dowiedzą się, jak przeprowadzać skany z uwierzytelnieniem i bez, rozumiejąc problemy związane z różnymi metodami uwierzytelniania.
2.4. Zapoznają się z technikami fuzzingu i wykorzystaniem dodatkowych payloadów.
2.5. Poznają zaawansowane narzędzia DAST drugiej generacji, takie jak Nuclei, oraz koncepcję Test-Driven Security.
2.6. Nauczą się, jak zintegrować podstawowy skan DAST z typowym potokiem CI/CD.
3. Analiza Składu (SCA) i łańcuch dostaw
3.1. Uczestnicy zgłębią problematykę podatnych bibliotek oraz kwestie niekompatybilnych licencji w procesie rozwoju oprogramowania.
3.2. Poznają koncepcję SBOM (Software Bill of Materials).

3.3. Dowiedzą się o różnicach między skanowaniem lokalnym a globalnym w kontekście SCA.
3.4. Zrozumieją istotę działań proaktywnych i retroaktywnych w zarządzaniu bezpieczeństwem komponentów.
3.5. Zapoznają się z zagrożeniami związanymi ze złośliwymi bibliotekami i atakami na łańcuch dostaw.
3.6. Nauczą się oceniać dojrzałość zależności, bibliotek i projektów.
3.7. Poznają różnice między narzędziami takimi jak OpenSSF, Packj i Guarddog.
3.8 Zgłębią koncepcję Provenance w kontekście standardu SLSA (Supply chain Levels for Software Artifacts).
4. Analiza Statyczna (SAST): Podstawy
4.1. Uczestnicy zgłębią problematykę sekretów w kodzie i poznają różne metody ich detekcji.
4.2. Nauczą się radzić sobie z fałszywymi pozytywnymi wynikami. Zrozumieją różnice między skanowaniem lokalnym a globalnym w kontekście wykrywania sekretów.
4.3. Poznają koncepcje proaktywnego i retroaktywnego podejścia do zarządzania sekretami.
4.4. Dowiedzą się, jak wykrywać sekrety nie tylko w kodzie, ale także w obrazach Docker i logach różnych narzędzi (CI, Slack).
4.5. Zapoznają się z procedurami rotacji sekretów i działaniami po ich wykryciu.
4.6. Na koniec poznają podstawy Statycznej Analizy Kodu (SAST) jako fundamentu podejścia „Secure by Default”.
5. Analiza Statyczna (SAST): Zaawansowane
5.1. Uczestnicy poznają podstawy skanowania SAST pierwszej generacji na przykładzie aplikacji webowej.
5.2. Zgłębią zaawansowane techniki SAST drugiej generacji, w tym wprowadzenie do narzędzia Semgrep.
5.3. Zapoznają się z przeglądem dostępnych narzędzi SAST obu generacji.

5.4. Zrozumieją różnice między skanami lokalnymi a globalnymi.
5.5. Poznają strategie efektywnego wdrażania SAST do procesu CI.
5.6. Nauczą się pisać własne reguły SAST, zarówno w wersji podstawowej, jak i z wykorzystaniem zaawansowanych technik.
5.7. Dowiedzą się, jak skanować pliki Infrastructure-as-Code i zastosować podejście Compliance-as-Code.
5.8. Zgłębią metody automatycznego skanowania podatności w klasycznej infrastrukturze.
6. Zarządzanie podatnościami
6.1. Uczestnicy zgłębią koncepcję zarządzania podatnościami (VM) w kontekście DevSecOps.
6.2. Poznają różnice między tradycyjnym podejściem do skanowania podatności a metodami stosowanymi w DevSecOps.
6.3. Dowiedzą się, jak ustalać i zarządzać SLA (Service Level Agreement) dla procesu eliminowania podatności.
6.4. Nauczą się budować własną bazę wiedzy (Knowledge Base) dotyczącą podatności i ich rozwiązywania.
6.5. Zgłębią różnice między oceną krytyczności podatności a oceną ryzyka, zrozumieją ich znaczenie w procesie priorytetyzacji działań naprawczych.

Załącznik B: Szczegółowa agenda programu “Ofensywne Testowanie Web Aplikacji”

1. Fundamenty cyberbezpieczeństwa
1.1. Podstawy działania sieci Web (HTTP, DOM, SOP, CORS).
1.2. Triada CIA i jej rozszerzenia.
1.3. CorpSec, NetSec, AppSec.
1.4. Sposoby oceny bezpieczeństwa aplikacji i systemów IT.
1.5. Testowanie Black-box, Gray-box i White-box.
2. Rekonesans i enumeracja
2.1. Uczestnicy odkryją stos technologiczny web aplikacji.
2.2. Wykonają skan web aplikacji pod kątem dostępnych zasobów i funkcjonalności.
2.3. Przeprowadzą automatyczny skan podatności web serwera.
2.4. Zweryfikują bezpieczeństwo certyfikatu SSL/TLS web aplikacji.
2.5. Wykonają aktywny podsłuch ruchu sieciowego.
2.6. Przeskanują aplikacje pod kątem używanego WAF-a.
3. Podatności w AuthZ i wstrzyknięcia kodu
3.1. Uczestnicy otrzymają dostęp do danych innych użytkowników dzięki podatności IDOR.
3.2. Wykradną ciasteczka użytkownika wykorzystując podatność XSS (symulacja realnego ataku).
3.3. Wykonają automatyczny skan podatności web aplikacji wykorzystując niestandardowe payloady (Fuzzing).
3.4. Zrozumieją istotę działań proaktywnych i retroaktywnych w zarządzaniu bezpieczeństwem komponentów.
4. Błędna logika, konfiguracja & podatne biblioteki

4.1. Uczestnicy poznają proces Modelowania Zagrożeń i pryncypia bezpiecznej architektury.
4.2. Zbadają bezpieczeństwo serwowanych przez aplikację nagłówków.
4.3. Wykonają automatyczny skan podatności używanych przez aplikację bibliotek (BE/FE).
4.4. Przeskanują obraz Dockerowy pod kątem bezpieczeństwa.
5. Podatności w AuthN, integralność & automatyzacja ataków
5.1. Uczestnicy przeprowadzą atak siłowy na hasło użytkownika web aplikacji.
5.2. Przeprowadzą atak “Credential Stuffing” na użytkowników web aplikacji.
5.3. Odkryją nowe podatności w aplikacji testowej dzięki automatyzacji (DAST).
5.4. Przeprowadzą zautomatyzowany atak na użytkowników usługi OpenSSH.
5.5. Wykonają symulację ataku na łańcuch dostawczy po stronie front-end (CDN).
6. Podatność SSRF i Raportowanie
6.1. Uczestnicy wykorzystają podatność, która spowodowała wielomilionowe ($$$) wycieki danych.
6.2. Poznają rynkowe narzędzia do oceny krytyczności oraz klasyfikacji znajdywanych podatności (CVE, CVSS, VRT).
6.3. Dowiedzą się w jaki sposób pisać wartościowy raport z testów bezpieczeństwa.

Załącznik C: Szczegółowa agenda programu “Praktyczne Modelowanie Zagrożeń”

1. Bezpieczeństwo w procesie wytwórczym (Secure SDLC, SSDLC)
1.1. Zarządzanie bezpieczeństwem aplikacji
1.2. Zarządzanie podatnościami
1.3. Budowanie wymagań bezpieczeństwa
1.4. Sposoby oceny bezpieczeństwa systemów IT
2. Modelowanie zagrożeń: Teoria
2.1. Poziomy modelowania zagrożeń
2.2. Podejście oparte o Attack Trees
2.3. Podejście oparte o model STRIDE
2.4. Rozszerzenie modelu STRIDE o model TRIM
2.5. Metodyka Agile Threat Modeling
2.6. Przegląd dostępnych narzędzi (TMT, Deciduous, Elevation of Privilege & Privacy, Cornucopia i inne)
3. Modelowanie zagrożeń: Praktyka
3.1. Modelowanie zagrożeń na poziomie infrastruktury - ćwiczenie
3.2. Modelowanie zagrożeń na poziomie aplikacji - ćwiczenie
3.3. Modelowanie zagrożeń na poziomie konkretnej funkcjonalności - ćwiczenie