Szkolenie: Mile2
C)SWAE - Certified Secure Web Application Engineer

Cel szkolenia:

Kurs Mile2 Certified Secure Web Application Engineer (CSWAE) przygotowuje programistów, inżynierów oprogramowania, specjalistów DevSecOps, zespoły ds. bezpieczeństwa aplikacji oraz menedżerów technicznych do projektowania, tworzenia i utrzymywania bezpiecznych aplikacji webowych. Uczestnicy poznają zasady bezpiecznego projektowania (secure design), modelowania zagrożeń (threat modeling), uwierzytelniania, autoryzacji, bezpiecznego zarządzania sesją i danymi, logowania, bezpiecznego wdrożenia, ochrony potoków CI/CD, bezpieczeństwa łańcucha dostaw oprogramowania (software supply chain security) oraz ochrony aplikacji w oparciu o analizę ryzyka w pełnym cyklu życia oprogramowania (SDLC).

Szkolenie CSWAE łączy również nowoczesne praktyki bezpieczeństwa aplikacji webowych ze standardem OWASP Top 10. Uczy uczestników, jak powstają zagrożenia – takie jak błędy kontroli dostępu (broken access control), podatności typu injection, błędne konfiguracje (misconfiguration), błędy kryptograficzne (cryptographic failures), słabości mechanizmów uwierzytelniania oraz zagrożenia w łańcuchu dostaw – a także jak im skutecznie zapobiegać. Podczas praktycznych laboratoriów na żywo, z wykorzystaniem narzędzi takich jak OWASP ZAP, uczestnicy weryfikują mechanizmy kontrolne, identyfikują podatności, doskonalą praktyki bezpiecznego wytwarzania oprogramowania oraz podnoszą realną gotowość do ochrony aplikacji w środowisku produkcyjnym.

Po ukończeniu szkolenia

- Po ukończeniu szkolenia uczestnicy będą wiedzieć, jak wspierać bezpieczne projektowanie, tworzenie, testowanie, wdrażanie oraz monitorowanie aplikacji webowych. Uczestnicy będą potrafili stosować zasady bezpiecznego kodowania (*secure coding*), ograniczać ryzyka na poziomie aplikacji oraz dostosowywać mechanizmy kontrolne do wytycznych OWASP i praktyk DevSecOps. Zdobędą również wiedzę niezbędną do przystąpienia do egzaminu certyfikacyjnego CSWAE.

Każdy uczestnik autoryzowanego szkolenia Mile2 C)SWAE realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin CSWAE Certified Secure Web Application Engineer.

Dla kogo przeznaczone jest szkolenie:

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Pentesterzy (*Pen Testers*)
- Oficerowie bezpieczeństwa / Security Officers
- Etyczni hakerzy (*Ethical Hackers*)
- Audytorzy sieciowi (*Network Auditors*)
- Analitycy ds. podatności (*Vulnerability Assessors*)
- Właściciele i menedżerowie systemów (*System Owners and Managers*)
- Inżynierowie ds. cyberbezpieczeństwa (*Cyber Security Engineers*)

Mile2® jest:

- ACCREDITED przez NSA CNSS 4011-4016 https://mile2.com/accreditations/
- MAPPED do NIST / Homeland Security NICCS Cyber Security Workforce Framework https://mile2.com/niccs/
- APPROVED na liście FBI Cyber Security Certification Requirement list (Tier 1-3)

Plan szkolenia:

- Moduł 01: Nastawienie na bezpieczeństwo, ryzyko i modelowanie zagrożeń
  - Nastawienie na bezpieczeństwo (*Security Mindset*)
  - Kluczowe zasady bezpieczeństwa
  - Myślenie w kategoriach ryzyka i założenia bezpiecznego projektowania (*Secure Design*)
  - Modelowanie zagrożeń z wykorzystaniem metodyki STRIDE
  - Zespołowa analiza ryzyka aplikacji
  - Budowanie kultury prewencji
- Moduł 02: Bezpieczne fundamenty: Architektura, warstwa transportowa i nagłówki
  - Bezpieczna architektura i granice zaufania (*Trust Boundaries*)
  - Segmentacja i koncepcja Zero Trust
  - Podstawy HTTPS i TLS
  - Zaufanie do certyfikatów i typowe zagrożenia dla TLS
  - Nagłówki bezpieczeństwa HTTP
  - Centralne zarządzanie nagłówkami
  - Rola lidera IT a bezpieczeństwo domyślne
- Moduł 03: Uwierzytelnianie i bezpieczeństwo sesji
  - Zasady uwierzytelniania
  - Typowe podatności w mechanizmach uwierzytelniania

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Higiena haseł i ich bezpieczne przechowywanie
- Uwierzytelnianie wieloskładnikowe (MFA)
- Protokoły OAuth 2.0 oraz OpenID Connect
- Zarządzanie sesją
- Bezpieczeństwo plików cookie
- Tokeny JWT i sesje oparte na tokenach
- Praktyki liderów w zakresie bezpieczeństwa tożsamości

- Moduł 04: Autoryzacja i kontrola dostępu
  - Zasady autoryzacji
  - Zasada minimalnych uprawnień (*Least Privilege*) oraz podział obowiązków (*Separation of Duties*)
  - Kontrola dostępu oparta na rolach (RBAC)
  - Kontrola dostępu oparta na atrybutach (ABAC)
  - Kontrola dostępu oparta na politykach (PBAC)
  - Błędy kontroli dostępu (*Broken Access Control*)
  - Bezpośrednie odwołania do obiektów (*Insecure Direct Object References – IDOR*)
  - Eskalacja uprawnień (*Privilege Escalation*)
  - Trwałość i egzekwowanie bezpiecznych zasad dostępu
- Moduł 05: Bezpieczne wprowadzanie i walidacja danych
  - Fundamenty bezpiecznego wprowadzania danych
  - Niezaufane źródła danych wejściowych
  - Walidacja, sanityzacja i kodowanie danych
  - Ataki Cross-Site Scripting (XSS)
  - Ataki typu Injection
  - Niebezpieczne przesyłanie plików (*Unsafe File Uploads*)
  - Deserializacja i zagrożenia związane z danymi strukturyzowanymi
  - Białe listy (*Allowlists*), normalizacja i walidacja schematów
  - Kodowanie danych wyjściowych zależne od kontekstu
  - Testowanie mechanizmów obronnych z wykorzystaniem OWASP ZAP
- Moduł 06: Bezpieczne przetwarzanie i przechowywanie danych
  - Identyfikacja danych wrażliwych
  - Poziomy klasyfikacji danych
  - Funkcje skrótu (hashing) a szyfrowanie
  - Nowoczesne metody haszowania haseł
  - Szyfrowanie danych w spoczynku (*Encryption at Rest*)
  - Tajemnice (*Secrets*), klucze i konfiguracja środowiskowa

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Typowe błędy w przechowywaniu danych
- Logowanie i buforowanie (*caching*) danych wrażliwych
- Minimalizacja danych i bezpieczne retencje
- Odpowiedzialność zespołowa i zarządcza za bezpieczeństwo danych

- Moduł 07: Monitorowanie, detekcja i logowanie
  - Dlaczego monitorowanie jest kluczowe
  - Logi, metryki i ślady (*Traces*)
  - Zasady prawidłowego logowania
  - Logowanie ustrukturyzowane vs. nieustrukturyzowane
  - Identyfikatory korelacji (*Correlation IDs*)
  - Metryki a kondycja systemu (*System Health*)
  - Śledzenie w systemach rozproszonych (*Distributed Tracing*)
  - Oddzielanie sygnału od szumu (*Signal vs. Noise*)
  - Typowe błędy w procesach logowania
  - Wykrywanie, alertowanie i widoczność operacyjna (*Operational Visibility*)
- Moduł 08: Bezpieczeństwo wdrożeń i zarządzanie konfiguracją
  - Dlaczego bezpieczeństwo wdrożeń jest kluczowe
  - Zasady bezpiecznej konfiguracji
  - Separacja środowisk
  - Minimalne uprawnienia dla usług i kontenerów
  - Zarządzanie sekretami (*Secrets Management*)
  - Pliki konfiguracyjne a zmienne środowiskowe
  - Zarządzanie poprawkami (*Patching*), zależnościami i kontrolą wersji
  - Typowe błędy konfiguracyjne (*Misconfigurations*)
  - Tryb debugowania, domyślne poświadczenia i wyeksponowane usługi
  - Walidacja konfiguracji i nadzór nad procesem wdrożenia (*Deployment Governance*)
- Moduł 09: Bezpieczny CI/CD i bezpieczeństwo łańcucha dostaw
  - Znaczenie bezpieczeństwa w potokach CI/CD
  - Powierzchnia ataku na procesy CI/CD
  - Minimalne uprawnienia w potokach wdrożeniowych (*Pipelines*)
  - Zaufanie do zależności i ich weryfikacja
  - Integralność artefaktów i autentyczność procesów budowania
  - SBOM (*Software Bill of Materials*) i widoczność łańcucha dostaw
  - Wykorzystanie sekretów w CI/CD
  - Uprzywilejowane i trwałe środowiska uruchomieniowe (*Build Runners*)
  - Utwardzanie (*Hardening*) i nadzór nad potokami CI/CD

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Bezpieczne przekazywanie kodu od repozytorium do środowiska produkcyjnego
- Moduł 10: Obsługa incydentów i przywracanie dostępności aplikacji webowych
  - Znaczenie sprawnego reagowania na incydenty
  - Rozpoznawanie incydentu bezpieczeństwa
  - Wykrycie a potwierdzenie incydentu
  - Cykl życia procesu reagowania na incydenty (*Incident Response Lifecycle*)
  - Ograniczanie skutków (*Containment*) bez niszczenia materiału dowodowego
  - Usuwanie skutków (*Eradication*) i przywracanie sprawności (*Recovery*)
  - Wyciąganie wniosków i analiza bez szukania winnych (*Blameless Review*)
  - Typowe niepowodzenia w reagowaniu na incydenty
  - Komunikacja i precyzyjny podział ról
  - Budowanie gotowości operacyjnej w zespołach deweloperskich
- Moduł 11: OWASP Top 10: Przekładanie ryzyka na praktykę
  - Cel i rola zestawienia OWASP Top 10
  - Najczęstsze błędy w interpretacji i stosowaniu OWASP Top 10
  - Podejście do standardu OWASP w ramach kursu
  - Błędy kontroli dostępu (*Broken Access Control*)
  - Błędy konfiguracji bezpieczeństwa (*Security Misconfiguration*)
  - Podatności w łańcuchu dostaw oprogramowania
  - Błędy kryptograficzne (*Cryptographic Failures*)
  - Ataki typu Injection
  - Niebezpieczne projektowanie (*Insecure Design*)
  - Błędy uwierzytelniania (*Authentication Failures*)
  - Naruszenia integralności oprogramowania i danych
  - Błędy w logowaniu i monitorowaniu
  - SSRF (*Server-Side Request Forgery*) oraz nowe zagrożenia aplikacji webowych
  - Mapowanie OWASP, przekładanie wytycznych na wymogi audytowe i podsumowanie warsztatów
- Lab 00: Wprowadzenie do środowiska laboratoryjnego
  - Rejestracja adresów IP i logowanie do systemu
- Lab 01: Modelowanie zagrożeń i podstawy bezpieczeństwa
  - Analiza aplikacji z perspektywy użytkownika niezalogowanego
  - Badanie aplikacji z pozycji użytkownika uwierzytelnionego
  - Modelowanie zagrożeń bez wykonywania eksploitacji
  - Obserwacja i testowanie założeń dotyczących zaufania za pomocą OWASP ZAP
  - Kategoryzacja i priorytetyzacja ryzyka

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Lab 02: Zabezpieczanie warstwy transportowej i nagłówków w aplikacji webowej
  - Pobranie aplikacji
  - Uruchomienie aplikacji za serwerem proxy Nginx
  - Generowanie lokalnego certyfikatu
  - Konfiguracja serwera Nginx pod kątem HTTPS i nagłówków
  - Uruchomienie środowiska
  - Weryfikacja nagłówków oraz konfiguracji TLS przy użyciu OWASP ZAP
  - Analiza wyników i dokumentacja wniosków
- Lab 03: Uwierzytelnianie i bezpieczeństwo sesji
  - Analiza stanu wyjściowego uwierzytelniania i obsługi sesji
  - Analiza plików cookie sesji
  - Identyfikacja ukrytych elementów (Score Board)
  - Ataki typu Injection w procesie uwierzytelniania
  - Analiza podatności w procedurze odzyskiwania konta
  - Ocena polityki haseł
  - Testowanie utrwalania (*Session Fixation*) i rotacji tokenów sesyjnych
- Lab 04: Autoryzacja i kontrola dostępu
  - Mapowanie powierzchni autoryzacji
  - Analiza bazowego zachowania mechanizmów autoryzacji
  - Autoryzacja pozioma (*Horizontal Authorization*)
  - Autoryzacja pionowa (*Vertical Authorization*)
  - Klasyfikacja: dostęp poziomy vs. pionowy
  - Definiowanie reguł autoryzacji
  - Tworzenie macierzy testów autoryzacji
  - Przegląd mechanizmów głębokiej ochrony (*Defense-in-Depth*)
- Lab 05: Operacja Czyste Wejście: Zabezpieczanie potoku danych
  - Zbieranie danych wywiadowczych: mapowanie punktów wejścia danych
  - Incydent "Pop-Up": badanie podatności XSS
  - "Wytrych" (*The Skeleton Key*): testowanie podatności na ataki Injection
  - "Koń Trojański": walidacja przesyłanych plików
  - "Tarcza Ochronna": mapowanie środków zaradczych (*Mitigation Mapping*)
  - Projekt: architektura głębokiej ochrony (*Defense-in-Depth*)
  - Kontrola końcowa: weryfikacja z użyciem OWASP ZAP
- Lab 06: Operacja Cichy Skarbiec: Zabezpieczanie danych w spoczynku i w tranzycie
  - Zbieranie danych wywiadowczych: mapowanie powierzchni przetwarzania danych
  - Wyciek z logów: identyfikacja ekspozycji danych tekstem jawnym (*Plaintext*)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Skarbiec poświadczeń: analiza metod haszowania haseł
- Zapomniany klucz: przegląd sekretów i konfiguracji
- Trojański plik: obsługa danych w przesyłanych plikach
- Projekt tarczy: mapowanie środków zaradczych poprzez wyzwania programistyczne (*Coding Challenges*)
- Protokół Skarbca: projektowanie głębokiej ochrony
- Audyt końcowy: weryfikacja z użyciem OWASP ZAP

- Lab 07: Operacja Szklany Dom: Oświetlanie ciemnych zakamarków
  - Zbieranie danych wywiadowczych: mapowanie powierzchni logowania
  - Wyciek sekretu: identyfikacja ekspozycji danych wrażliwych
  - Ściana szumu: analiza relacji sygnału do szumu
  - Przerwany ślad: korelacja i kontekst zdarzeń
  - Projekt tarczy: mapowanie środków zaradczych
  - Protokół widoczności: projektowanie polityki logowania
  - Audyt końcowy: symulacja weryfikacyjna
- Lab 08: Operacja Utwardzona Powłoka: Zabezpieczanie wdrożeń i konfiguracji
  - Zbieranie danych wywiadowczych: mapowanie powierzchni kontenerów
  - Furtka debugowania: naddatkowa ekspozycja błędów (*Verbose Errors*)
  - Wyciek sekretu: poszukiwanie zakodowanych na stałe poświadczeń (*Hardcoded Credentials*)
  - Ryzyko konta Root: testowanie zasady minimalnych uprawnień
  - Projekt tarczy: mapowanie środków zaradczych
  - Fortyfikacja: utwardzanie środowiska wdrożeniowego (*Hardening*)
  - Audyt końcowy: weryfikacja z użyciem OWASP ZAP
- Lab 09: Operacja Zaufana Fabryka: Zabezpieczanie łańcucha dostaw
  - Inspekcja artefaktów: analiza warstw i historii zmian
  - Wyciek sekretu: ekspozycja logów i konfiguracji CI
  - Zaufanie do zależności: analiza podatnych bibliotek
  - Integralność artefaktów: haszowanie i weryfikacja
  - Projekt tarczy: mapowanie środków zaradczych
  - Protokół potoku: projektowanie polityki bezpieczeństwa CI/CD
  - Audyt końcowy: symulacja weryfikacyjna
- Lab 10: Operacja Spokojne Centrum: Reagowanie na incydenty i odzyskiwanie sprawności
  - Detekcja i analiza: oddzielanie sygnału od szumu
  - Zgłoszenie i formalna komunikacja
  - Ograniczanie skutków (*Containment*): zatrzymanie incydentu
  - Zabezpieczanie materiału dowodowego

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Przywracanie sprawności i weryfikacja
- Wnioski i analiza po incydencie (*Lessons Learned*)

Wymagania:

Sugerowane wymagania wstępne:

- Ugruntowana wiedza z zakresu sieci komputerowych
- Znajomość przynajmniej jednego języka programowania
- Znajomość systemu Linux
- Umiejętność pracy w terminalu (open shell)

lub 24 miesiące doświadczenia w obszarze technologii programistycznych i bezpieczeństwa

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę Mile2.

Ponadto kurs ten przygotowuje uczestników do certyfikowanego egzaminu Certified Secure Web Application Engineer CSWAE, który jest realizowany za pośrednictwem systemu egzaminacyjnego Mile2’s Learning Management System, z poziomu konta mile2.com. Egzamin trwa około 2 godzin i składa się ze 100 pytań wielokrotnego wyboru. Aby uzyskać certyfikację, wymagany jest wynik co najmniej 70%.

Each participant in an authorized Mile2 C)SWAE training held in Compendium CE will receive a free CSWAE Certified Secure Web Application Engineer exam voucher.

Prowadzący:

Autoryzowany instruktor Mile2 (Certified Mile2 Instructor).

Informacje dodatkowe:

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Pakiet uczestnika szkolenia (Course Student Kit) obejmuje:

- Digital Workbook & Study Guide – materiały szkoleniowe w wersji elektronicznej (roczny dostęp)
- Live Cyber Range Labs – środowisko laboratoryjne dostępne w chmurze (2 tygodniowy dostęp)
- Exam Prep Guide + Practice Questions – dodatowe materiały przygotowujące do egzaminu
- Official Certification Exam (2 Attempts Included) – voucher egzaminacyjny wraz drugi darmowym podejściem jeżeli byłoby potrzebne

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001