SZKOLENIE ŚREDNIO ZAAWANSOWANE

OSINT dla cyberbezpieczeństwa – zobacz swoją firmę oczami atakującego

SEC/OSINT

Czas trwania: 2 dni (16h)

Sprawdź, co cyberprzestępcy mogą dowiedzieć się o Twojej firmie. Poznaj techniki OSINT, analizuj powierzchnię ataku i wykrywaj zagrożenia, zanim wykorzystają je napastnicy.

Cele szkolenia

- Szkolenie wyjaśnia rolę OSINT (Open Source Intelligence) w nowoczesnym cyberbezpieczeństwie oraz jego zastosowanie w identyfikacji zagrożeń
- Szkolenie przedstawia sposób, w jaki atakujący prowadzą rekonesans i wykorzystują informacje publiczne do przygotowania ataków
- Szkolenie uczy rozróżniania rekonesansu pasywnego i aktywnego oraz poznania prawnych i etycznych granic OSINT
- Szkolenie rozwija umiejętność identyfikowania informacji o organizacji dostępnych publicznie w internecie
- Szkolenie uczy oceny własnej powierzchni ataku z perspektywy potencjalnego przeciwnika
- Szkolenie pokazuje, jak wykrywać nadmierną ekspozycję informacji firmowych, w tym kluczy API i haseł w publicznych repozytoriach kodu
- Szkolenie pomaga rozpoznawać zagrożenia związane z mediami społecznościowymi i publikowaniem informacji o firmie oraz jej pracownikach
- Szkolenie przedstawia metody monitorowania wycieków danych i ujawnionych informacji dotyczących organizacji
- Szkolenie przygotowuje do ograniczania ryzyka związanego z OSINT poprzez identyfikację podatności informacyjnych i właściwe zarządzanie ekspozycją
- Szkolenie wspiera budowanie świadomości pracowników w zakresie bezpiecznego publikowania informacji w internecie

Zalety

- Uczestnik analizuje organizację z perspektywy potencjalnego atakującego, wykorzystując techniki OSINT i publicznie dostępne źródła informacji
- Uczestnik łączy wiedzę z zakresu OSINT, cyberbezpieczeństwa i zarządzania ryzykiem w celu identyfikacji zagrożeń
- Uczestnik rozpoznaje prawne i etyczne granice pracy z OSINT, w tym zasady autoryzacji działań i ochrony danych osobowych
- Uczestnik identyfikuje źródła i narzędzia OSINT wykorzystywane do rekonesansu organizacji oraz analizy jej infrastruktury
- Uczestnik analizuje przypadki związane z ekspozycją informacji i ocenia ryzyko na podstawie ćwiczeń warsztatowych oraz doświadczenia prowadzącego
- Uczestnik wykrywa potencjalne problemy związane z publicznym ujawnieniem informacji firmowych i formułuje rekomendacje ograniczające ryzyko ich wykorzystania przez napastników
- Uczestnik wykorzystuje wiedzę z zakresu OSINT do identyfikacji zagrożeń istotnych dla działów IT, bezpieczeństwa oraz kadry zarządzającej

Dla kogo?

- Specjaliści cyberbezpieczeństwa
- Administratorzy IT i systemów
- Zespoły SOC i osoby odpowiedzialne za monitoring zagrożeń

- Audytorzy bezpieczeństwa informacji
- Administratorzy odpowiedzialni za ekspozycję usług internetowych
- Kadra kierownicza odpowiedzialna za bezpieczeństwo organizacji
- Pracownicy IT odpowiedzialni za zarządzanie ryzykiem w organizacji

Wymagania

- Znajomość podstaw cyberbezpieczeństwa
- Podstawowa znajomość działania internetu i usług sieciowych
- Umiejętność korzystania ze standardowych wyszukiwarek internetowych

Program

1. Wprowadzenie do OSINT
2. Czym jest Open Source Intelligence
3. OSINT jako element cyberbezpieczeństwa
4. Kiedy informacja dostępna publicznie staje się ryzykiem
5. Jak atakujący wykorzystują informacje dostępne online: rekonesans w ujęciu MITRE ATT&CK
6. Prawne i etyczne granice OSINT
7. Rekonesans pasywny i aktywny: czym się różnią i dlaczego ma to skutki prawne
8. Aktywne testowanie cudzej infrastruktury, w szczególności skanowanie usług, odbywa się wyłącznie w uzgodnionym zakresie i na podstawie odpowiedniego upoważnienia; dopuszczalność konkretnych działań zależy od ich charakteru i okoliczności
9. Zasady prowadzenia warsztatów: działania ingerujące w infrastrukturę są wyłączone, chyba że zostały wcześniej wyraźnie uzgodnione i autoryzowane
10. Granice legalnego postępowania z danymi uwierzytelniającymi ujawnionymi w wycieku: zakaz nieuprawnionych prób dostępu, bezpieczne zgłaszanie znalezisk oraz omówienie przepisów Kodeksu karnego, w tym art. 267 i 269b, w zakresie właściwym dla omawianych przypadków (wyłączenie z art. 269b § 1a dotyczy działań podejmowanych wyłącznie w celu zabezpieczenia systemu lub opracowania metody takiego zabezpieczenia, w granicach określonych w przepisie; nie legalizuje ono dowolnego gromadzenia znalezionych danych uwierzytelniających)
11. RODO w OSINT: analiza profili pracowników to przetwarzanie danych osobowych – ustalenie odpowiedniej podstawy prawnej, realizacja obowiązku informacyjnego oraz ograniczenie zakresu przetwarzanych danych
12. Zasady etyczne i autoryzacja: ustalony zakres, zgoda właściciela, dokumentowanie działań, praca na organizacji fikcyjnej lub za zgodą
13. Organizacja oczami atakującego
14. Budowanie profilu organizacji
15. Identyfikacja technologii wykorzystywanych przez firmę
16. Określanie potencjalnych punktów wejścia
17. Tworzenie mapy powierzchni ataku
18. OSINT jako etap testów penetracyjnych i ćwiczeń Red Team: za zgodą i w ustalonym zakresie
19. OSINT dotyczący pracowników
20. Media społecznościowe jako źródło informacji
21. Ryzyko nieświadomej publikacji informacji
22. Analiza stanowisk i ról w organizacji
23. Identyfikacja osób kluczowych dla ataku
24. Zasady publikacji informacji o pracy i firmie, które organizacja może przekazać pracownikom
25. Analiza infrastruktury i usług internetowych
26. Domeny i subdomeny: źródła pasywne (m.in. certyfikaty, historyczne dane DNS) a aktywna enumeracja
27. Publiczne usługi organizacji i informacje techniczne dostępne w internecie
28. Niebezpieczne ujawnienia konfiguracji
29. Publicznie dostępne zasoby w chmurze, np. niezabezpieczone zasobniki obiektowe (m.in. zasobniki Amazon S3)
30. Konfiguracja SPF, DKIM i DMARC: wykrywanie brakujących lub błędnych ustawień oraz ich znaczenie dla ryzyka podszywania się pod nadawcę
31. Znaczenie higieny informacji technicznych
32. Wycieki danych i ekspozycja informacji
33. Typy wycieków danych
34. Ujawnione konta i hasła: jak sprawdzać własne domeny i konta bez naruszania prawa
35. Klucze API, hasła i pliki konfiguracyjne w publicznych repozytoriach kodu (np. GitHub, GitLab)
36. Monitorowanie informacji o organizacji
37. Reakcja na znalezienie własnych danych: unieważnienie kluczy i haseł, ocena, czy doszło do naruszenia ochrony danych
38. Znaczenie procedur podstawowego bezpieczeństwa
39. OSINT wykorzystywany przez cyberprzestępców
40. Rekonesans przed phishingiem, w tym phishing ukierunkowany na konkretne osoby
41. Przygotowanie wiarygodnych wiadomości
42. Identyfikacja dostawców i partnerów
43. Ataki socjotechniczne oparte na informacjach publicznych
44. Łączenie wielu źródeł informacji

45. OSINT po stronie obrony
46. Własny monitoring ekspozycji organizacji
47. Threat Intelligence
48. Wczesne wykrywanie zagrożeń, np. fałszywych domen podszywających się pod firmę
49. Monitoring ekspozycji jako element zarządzania ryzykiem, w tym ryzykiem w łańcuchu dostaw (kontekst NIS2; zakres obowiązków zależy od statusu organizacji)
50. Zwiększanie świadomości organizacji w zakresie informacji dostępnych publicznie
51. Narzędzia i metody pracy OSINT
52. Wyszukiwanie zaawansowane: operatory wyszukiwarek (tzw. Google dorking)
53. Certyfikaty i dane rejestracyjne domen: Certificate Transparency (np. crt.sh), WHOIS i RDAP (zakres publikowanych danych rejestracyjnych, w tym ograniczenia dotyczące danych osobowych abonentów domen .pl), archiwa stron (Wayback Machine)
54. Wyszukiwarki urządzeń i usług dostępnych w internecie (np. Shodan, Censys)
55. Sprawdzanie własnych kont i domen w usługach informujących o wyciekach (np. Have I Been Pwned): weryfikacja własności domeny, bezpieczne postępowanie ze znalezionymi danymi, zakaz wpisywania prawdziwych haseł firmowych do dowolnych serwisów
56. Analiza metadanych plików (np. exiftool)
57. Publiczne rejestry i ogłoszenia (np. KRS, CEIDG, oferty pracy)
58. Automatyzacja zbierania informacji i platformy agregujące (np. SpiderFoot, Maltego): możliwości, ograniczenia oraz różnica między operacjami korzystającymi z już zebranych danych a bezpośrednio kontaktującymi się z infrastrukturą celu; na warsztatach używane są wyłącznie moduły pasywne
59. Ocena wiarygodności źródeł i dokumentowanie ustaleń
60. Warsztaty praktyczne
61. Analiza publicznych informacji o organizacji fikcyjnej lub udostępnionej za zgodą, wyłącznie z użyciem metod rekonesansu pasywnego i publicznie dostępnych źródeł
62. Budowanie profilu organizacji będącej potencjalnym celem ataku, bez profilowania rzeczywistych osób
63. Mapa powierzchni ataku: identyfikacja informacji, domen, usług i technologii dostępnych publicznie
64. Ocena i priorytetyzacja zidentyfikowanych ryzyk
65. Prezentacja wyników przez grupy i omówienie ich w gronie uczestników
66. Przygotowanie rekomendacji ograniczających ekspozycję