SZKOLENIE ŚREDNIO ZAAWANSOWANE

Zarządzanie podatnościami w praktyce – od znalezienia błędu do jego usunięcia

SEC/VM

Czas trwania: 2 dni (16h)

Szkolenie prezentuje praktyczne zarządzanie podatnościami w organizacji: vulnerability management od wykrycia luk, analizy CVE i CVSS oraz oceny ryzyka, przez priorytetyzację, patch management i obsługę wyjątków, po weryfikację usunięcia podatności, raportowanie bezpieczeństwa i wsparcie zgodności z wymaganiami NIS2

Cele szkolenia

- Szkolenie przygotowuje do organizowania procesu zarządzania podatnościami w organizacji – od identyfikacji luki bezpieczeństwa, przez ocenę ryzyka, po potwierdzenie jej usunięcia lub ograniczenia ryzyka
- Szkolenie uczy analizowania podatności z uwzględnieniem CVE, CVSS, EPSS, kontekstu biznesowego i operacyjnego oraz ustalania priorytetów działań naprawczych
- Szkolenie pokazuje zasady planowania, testowania i wdrażania poprawek bezpieczeństwa w ramach patch management, z uwzględnieniem ciągłości działania systemów i usług
- Szkolenie przygotowuje do dokumentowania wyjątków w zarządzaniu podatnościami, stosowania środków kompensacyjnych oraz prowadzenia uzasadnionej akceptacji ryzyka
- Szkolenie rozwija umiejętność raportowania stanu podatności, komunikowania ryzyka cyberbezpieczeństwa kierownictwu oraz współpracy między IT, bezpieczeństwem i biznesem

Zalety

- Uczestnik analizuje raporty ze skanowania podatności i identyfikuje luki wymagające pilnej reakcji, w tym fałszywe alarmy i duplikaty
- Uczestnik ocenia ryzyko związane z podatnościami na podstawie CVSS, EPSS, katalogu CISA KEV, ekspozycji systemów i kontekstu biznesowego
- Uczestnik planuje działania naprawcze w ramach patch management i ustala priorytety oraz terminy wdrażania poprawek zgodnie z przyjętymi SLA
- Uczestnik dokumentuje wyjątki od usuwania podatności, dobiera środki kompensacyjne i uzasadnia akceptację ryzyka
- Uczestnik weryfikuje usunięcie podatności poprzez ponowne skanowanie, analizę wyników i ocenę skuteczności działań naprawczych
- Uczestnik raportuje stan zarządzania podatnościami, wykorzystując metryki bezpieczeństwa, oraz komunikuje ryzyko zespołom IT, właścicielom systemów i kierownictwu

Dla kogo?

- Specjaliści cyberbezpieczeństwa odpowiedzialni za wykrywanie, analizę i obsługę podatności w organizacji
- Administratorzy systemów, sieci i chmury z podstawową znajomością infrastruktury IT i utrzymania środowisk
- Zespoły IT i DevOps realizujące aktualizacje, zmiany oraz działania naprawcze w systemach i aplikacjach
- Administratorzy i właściciele aplikacji odpowiadający za bezpieczeństwo, dostępność i ciągłość działania usług
- Audytorzy, analitycy ryzyka i osoby ds. compliance uczestniczące w ocenie ryzyka oraz zgodności z wymaganiami
- Kierownicy IT, bezpieczeństwa i właściciele systemów biznesowych podejmujący decyzje o priorytetach i akceptacji ryzyka

Wymagania

- Podstawowa znajomość infrastruktury IT
- Podstawowa wiedza dotycząca cyberzagrożeń
- Znajomość podstaw działania systemów operacyjnych i aplikacji
- Mile widziane doświadczenie w administracji IT lub bezpieczeństwie

Program

1. Podstawy zarządzania podatnościami
2. Czym jest podatność bezpieczeństwa
3. Podatność, zagrożenie i ryzyko – różnice
4. Dlaczego podatności powstają
5. Typowy cykl życia podatności: od powstania, przez ujawnienie i publikację poprawki, po wykorzystanie w atakach
6. Proces zarządzania podatnościami: inwentaryzacja, wykrywanie, ocena, priorytetyzacja, naprawa, weryfikacja, raportowanie
7. Role i odpowiedzialność w procesie: bezpieczeństwo, IT, właściciele systemów, zarząd
8. Inwentaryzacja aktywów i powierzchnia ataku
9. Dlaczego bez wiedzy o tym, co jest w organizacji, nie da się zarządzać podatnościami
10. Zakres inwentarza: serwery, stacje robocze, urządzenia sieciowe, aplikacje, zasoby w chmurze i usługi SaaS, kontenery
11. Zasoby poza kontrolą IT (shadow IT) i zapomniane systemy
12. Krytyczność aktywów i ich właściciele
13. Zarządzanie powierzchnią ataku: jakie systemy są widoczne z internetu
14. Systemy po zakończeniu wsparcia producenta (EOL)
15. Źródła informacji o podatnościach
16. Identyfikatory CVE oraz bazy podatności (NVD, EUVD): czym różni się system identyfikatorów od baz, które wzbogacają wpisy o dodatkowe dane (CVSS, CWE, CPE)
17. Jak powstaje CVE: program prowadzony przez MITRE, identyfikatory nadają organizacje CNA (w Polsce m.in. CERT Polska); ENISA pełni rolę CVE Root dla podmiotów europejskich
18. Zmiany w NVD od kwietnia 2026 r.: wzbogacanie w pierwszej kolejności podatności z katalogu CISA KEV, oprogramowania używanego w administracji federalnej USA i oprogramowania krytycznego; pozostałe mają status „Not Scheduled”, a NVD zwykle nie dodaje własnej oceny dotkliwości, gdy podał ją CNA – skutki dla narzędzi opartych na danych NVD
19. Europejska baza podatności EUVD prowadzona przez ENISA (od 2025 r.): zestawienia podatności krytycznych, wykorzystywanych i koordynowanych w UE oraz znaczenie w kontekście NIS2
20. System CVSS (wersje 3.1 i 4.0): co ocena krytyczności mówi, a czego nie mówi
21. Jak czytać wynik CVSS 4.0: ocena bazowa (CVSS-B) a oceny uwzględniające zagrożenie i środowisko (CVSS-BT, CVSS-BE, CVSS-BTE); publikowane oceny są zwykle tylko bazowe
22. Biuletyny i poradniki bezpieczeństwa producentów oraz dane o wpływie podatności na produkt (CSAF, VEX)
23. Źródła krajowe i sektorowe: CERT Polska, CSIRT NASK i CSIRT-y sektorowe
24. Informacje o zagrożeniach (threat intelligence)
25. Wykrywanie podatności
26. Skanowanie infrastruktury IT: skany uwierzytelnione i nieuwierzytelnione, zakres i wpływ na działanie systemów
27. Podatności systemów operacyjnych, aplikacji i urządzeń sieciowych
28. Błędy konfiguracji i ich wykrywanie na podstawie wzorców konfiguracji (np. CIS Benchmarks)
29. Podatności w komponentach i bibliotekach: analiza składu oprogramowania (SCA), wykaz komponentów (SBOM), obrazy kontenerów i kod infrastruktury (IaC)
30. Różnica między automatycznym skanem a realną oceną ryzyka
31. Analiza raportów skanerów: fałszywe alarmy, duplikaty, podatności niewykryte przez skaner
32. Ocena i priorytetyzacja ryzyka
33. Dlaczego CVSS nie wystarcza: wskazuje dotkliwość podatności, a nie ryzyko dla konkretnej organizacji
34. Prawdopodobieństwo wykorzystania podatności: EPSS
35. Podatności aktywnie wykorzystywane w atakach: katalog CISA KEV i zestawienie podatności wykorzystywanych w EUVD
36. Modele decyzyjne, np. SSVC (Stakeholder-Specific Vulnerability Categorization)
37. Kontekst biznesowy: krytyczność aktywów, ekspozycja na internet, dostępne środki kompensacyjne
38. Tworzenie kolejności działań naprawczych i zasad priorytetyzacji możliwych do zastosowania w organizacji
39. Zarządzanie poprawkami bezpieczeństwa
40. Patch management
41. Testowanie aktualizacji
42. Ryzyko związane z brakiem poprawek i z niekontrolowaną zmianą
43. Planowanie wdrożeń, okna serwisowe, możliwość wycofania zmiany
44. Terminy naprawy (SLA) zależne od priorytetu: jak je ustalać, kto za nie odpowiada i jak je egzekwować
45. Tryb awaryjny: zero-day i podatności aktywnie wykorzystywane, gdy standardowy cykl testów jest zbyt wolny

(emergency patching)
46. Rozwiązania tymczasowe: wyłączenie usługi, ograniczenie dostępu, reguły zapory, wirtualne łatanie
47. Sprawdzenie, czy przed załataniem nie doszło do włamania
48. Podatności w środowiskach firmowych
49. Systemy Windows i Linux
50. Aplikacje biznesowe
51. Urządzenia sieciowe i brzegowe (VPN, zapory, bramy dostępowe)
52. Chmura i usługi SaaS: podział odpowiedzialności między dostawcę a organizację
53. Urządzenia użytkowników końcowych
54. Zarządzanie wyjątkami i akceptacją ryzyka
55. Kiedy podatności nie można natychmiast usunąć
56. Dokumentowanie wyjątków
57. Okres ważności wyjątku i cykliczny przegląd: dlaczego wyjątki bezterminowe są błędem
58. Środki kompensacyjne
59. Odpowiedzialność właścicieli systemów i osoby akceptującej ryzyko
60. Weryfikacja i raportowanie
61. Potwierdzanie usunięcia podatności
62. Ponowne skanowanie
63. Raportowanie stanu bezpieczeństwa
64. Metryki dla działu IT i zarządu, np. średni czas usunięcia (MTTR), zgodność z terminami naprawy, wiekowanie podatności, pokrycie skanowaniem
65. Budowanie świadomości ryzyka
66. Integracja z procesami bezpieczeństwa i wymaganiami prawnymi
67. Podatności a zarządzanie incydentami
68. Podatności a audyty bezpieczeństwa
69. Podatności a wymagania NIS2 i ustawy o KSC: obsługa i ujawnianie podatności jako jeden ze środków zarządzania ryzykiem (art. 21 ust. 2 lit. e dyrektywy NIS2)
70. Skoordynowane ujawnianie podatności (CVD): zgłaszanie podatności znalezionych u dostawców i przyjmowanie zgłoszeń od zewnętrznych badaczy
71. Rozporządzenie o cyberodporności (CRA): obowiązek producentów zgłaszania aktywnie wykorzystywanych podatności obowiązujący od 11 września 2026 r. i co to zmienia dla użytkowników produktów
72. Warsztaty praktyczne
73. Analiza przykładowego raportu podatności, w tym rozpoznawanie fałszywych alarmów
74. Ocena poziomu ryzyka z wykorzystaniem CVSS, EPSS, katalogu KEV i kontekstu biznesowego
75. Ustalenie priorytetów naprawy i terminów (SLA)
76. Decyzja o wyjątku z okresem ważności i środkami kompensacyjnymi
77. Scenariusz awaryjny: nowa podatność aktywnie wykorzystywana w urządzeniu dostępnym z internetu
78. Przygotowanie planu działań i metryk dla zarządu
79. Dyskusja nad decyzjami