Szkolenie Blue Team w praktyce: Zabezpieczenia punktów końcowych i zgodność z Microsoft Intune i Defender

Opis szkolenia: Szkolenie ma na celu zapoznanie uczestników z Microsfoft Defender i Microsoft Defender oraz wprowadzenie w tematykę Blue Team.

Kod szkolenia: BLUE-TEAM-01

Kategoria: Blue Team

Trenerka: Beata Zalewa

Czas trwania: 24 godziny (9:00 – 17:00)

Język wykładowy: język polski

Forma szkolenia: zdalne. Po wcześniejszym uzgodnieniu możliwe szkolenie w siedzibie klienta.

Materiały i narzędzia: w języku angielskim. Na życzenie klienta materiały w języku polskim.

Wymagania wstępne: Podstawowa znajomość zagadnień związanych z bezpieczeństwem. Uczestnicy otrzymają zestaw danych testowych i materiałów (skrypty, linki). Podczas szkolenia będą korzystali z własnych komputerów i licencji.

Grupa decelowa:

- Specjaliści ds. bezpieczeństwa IT i administratorzy systemów
- Inżynierowie ds. zgodności i zarządzania urządzeniami
- Architekci rozwiązań chmurowych i DevSecOps
- Osoby odpowiedzialne za wdrażanie polityk bezpieczeństwa w organizacji
- Zespoły SOC i Blue Team

Cel szkolenia: Nabycie umiejętności skutecznego zarządzania urządzeniami i aplikacjami w środowisku Microsoft 365, wdrażania i egzekwowania zasad bezpieczeństwa z użyciem Intune i Defender. Reagowania na incydenty i analizowania zagrożeń w czasie rzeczywistym. Zapewnienia zgodności z przepisami i standardami branżowymi oraz projektowania strategii bezpieczeństwa opartej na najlepszych praktykach Blue Team.

Efekty szkolenia:

- Uczestnik zna zaawansowaną architekturę i funkcjonalności systemów Microsoft Intune oraz Microsoft Defender, a także zasady działania mechanizmów wykrywania i reagowania na zagrożenia na punktach końcowych (EDR).
- Uczestnik potrafi samodzielnie konfigurować, wdrażać i egzekwować polityki bezpieczeństwa oraz profile zgodności (compliance) dla urządzeń końcowych w organizacji z poziomu chmurowej konsoli zarządzającej.

- Uczestnik potrafi skutecznie monitorować alerty bezpieczeństwa, analizować wektory ataków na stacje robocze oraz przeprowadzać procedury izolacji i neutralizacji zagrożeń w ramach codziennych operacji defensywnych (Blue Team).
- Uczestnik rozumie praktyczne zastosowanie filozofii Zero Trust (Nigdy nie ufaj, zawsze weryfikuj) w obszarze zarządzania tożsamością i stanem technicznym urządzeń uzyskujących dostęp do zasobów firmy.
- Uczestnik rozumie znaczenie ciągłego utrzymywania zgodności konfiguracji systemowej oraz korelacji zdarzeń bezpieczeństwa dla zapewnienia integralności i cyfrowej odporności całej infrastruktury IT.

Co otrzymasz?

- Materiały szkoleniowe.
- Szkolenie kończy się certyfikatem uczestnictwa.

Agenda szkolenia

Dzień 1: Podstawy bezpieczeństwa punktów końcowych z Microsoft Intune

Godzina	Czas trwania	Moduł	Forma
9:00 – 9:15	15 minut	Moduł 1: Wprowadzenie do szkolenia i celów Blue Team	Prezentacja, dyskusja
9:15 – 10:45	90 minut	Moduł 2: Microsoft Intune – architektura, wdrożenie i zarządzanie urządzeniami	Teoria, demo, laboratorium
10:45 – 11:00	15 minut	Przerwa	–
11:00 – 13:00	120 minut	Moduł 3: Konfiguracja zasad bezpieczeństwa i zgodności	Teoria, laboratorium
13:00 – 13:30	30 minut	Przerwa obiadowa	–
13:30 – 15:00	90 minut	Moduł 4: Zasady ASR (Attack Surface Reduction) – projektowanie i wdrażanie	Teoria, laboratorium

Godzina	Czas trwania	Moduł	Forma
15:00 – 15:15	15 minut	Przerwa	–
15:15 – 16:45	90 minut	**Moduł 5: Wykluczenia ASR i zarządzanie wyjątkami**	Laboratorium
16:45 – 17:00	15 minut	**Sesja Q&A**	Pytania

Dzień 2: Ochrona danych i aplikacji mobilnych

Godzina	Czas trwania	Moduł	Forma
9:00 – 9:15	15 minut	**Podsumowanie dnia pierwszego**	Podsumowanie
9:15 – 10:30	75 minut	**Moduł 6: Zarządzanie aplikacjami mobilnymi (MAM) – podejście zarządzane i BYOD**	Teoria, laboratorium
10:30 – 10:45	15 minut	Przerwa	–
10:45 – 12:30	105 minut	**Moduł 7: Czyszczenie danych i kontrola dostępu**	Teoria, laboratorium
12:30 – 13:00	30 minut	Przerwa obiadowa	–
13:00 – 15:00	120 minut	**Moduł 8: Microsoft Defender for Endpoint – integracja z Intune**	Teoria, laboratorium
15:00 – 15:15	15 minut	Przerwa	–
15:15 – 16:45	90 minut	**Moduł 9: Scenariusze reagowania na incydenty i analiza alertów**	Teoria, laboratorium
16:45 – 17:00	15 minut	**Sesja Q&A**	Pytania

Dzień 3: Zgodność, ochrona chmury i strategia bezpieczeństwa

Godzina	Czas trwania	Moduł	Forma
9:00 – 9:15	15 minut	Podsumowanie dnia drugiego	Podsumowanie
9:15 – 10:30	75 minut	Moduł 10: Microsoft Defender for Cloud – zabezpieczanie usług utworzonych w chmurze Azure	Teoria, laboratorium
10:30 – 10:45	15 minut	Przerwa	–
10:45 – 12:30	105 minut	Moduł 11: Kontrole zgodności i raportowanie	Teoria, laboratorium
12:30 – 13:00	60 minut	Przerwa obiadowa	–
13:00 – 15:00	120 minut	Moduł 12: Tworzenie polityk bezpieczeństwa i ich egzekwowanie	Teoria, laboratorium
15:00 – 15:15	15 minut	Przerwa	–
15:15 – 16:45	90 minut	Moduł 13: Przegląd innych rodzajów Defenderów	Teoria, laboratorium
16:45 – 17:00	15 minut	Moduł 14: Podsumowanie i sesja pytań	Q&A, ankieta końcowa

Szczegółowy program szkolenia

Moduł 1: Wprowadzenie do szkolenia i celów Blue Team

- Omówienie celów szkolenia, roli zespołów Blue Team w organizacji
- Przegląd narzędzi Microsoft wykorzystywanych w programie.

Moduł 2: Microsoft Intune – architektura, wdrożenie i zarządzanie urządzeniami

- Wprowadzenie do Intune jako centralnego narzędzia do zarządzania punktami końcowymi.

- Uczestnicy poznają architekturę, scenariusze wdrożeniowe i podstawowe funkcje zarządzania urządzeniami.

Moduł 3: Konfiguracja zasad bezpieczeństwa i zgodności

- Tworzenie i egzekwowanie zasad zgodności dla urządzeń firmowych i prywatnych.
- Uczestnicy nauczą się konfigurować profile zabezpieczeń i monitorować ich skuteczność.

Moduł 4: Zasady ASR – projektowanie i wdrażanie

- Zasady redukcji powierzchni ataku (ASR) jako kluczowy element ochrony punktów końcowych.
- Praktyczne wdrożenie zasad i analiza ich wpływu na środowisko.

Moduł 5: Wykluczenia ASR i zarządzanie wyjątkami

- Zaawansowane scenariusze zarządzania wyjątkami – dodawanie wykluczeń dla plików wykonywalnych, urządzeń i aplikacji.
- Praktyczne podejście do równoważenia bezpieczeństwa i funkcjonalności.

Moduł 6: Zarządzanie aplikacjami mobilnymi (MAM)

- Zarządzanie aplikacjami na urządzeniach zarządzanych i niezarządzanych (BYOD).
- Konfiguracja zasad ochrony danych i kontrola dostępu do aplikacji firmowych.

Moduł 7: Czyszczenie danych i kontrola dostępu

- Symulacja scenariuszy, w których konieczne jest usunięcie danych firmowych z urządzeń użytkowników bez naruszania danych prywatnych.

Moduł 8: Microsoft Defender for Endpoint – integracja z Intune

- Zintegrowane podejście do ochrony punktów końcowych.
- Uczestnicy poznają sposób działania Defendera i jego integrację z Intune w celu wykrywania i reagowania na zagrożenia.

Moduł 9: Scenariusze reagowania na incydenty i analiza alertów

- Ćwiczenia praktyczne z wykorzystaniem alertów bezpieczeństwa, analiza incydentów i podejmowanie decyzji w czasie rzeczywistym.

Moduł 10: Microsoft Defender for Cloud – zabezpieczanie usług utworzonych w chmurze Azure

- Ochrona środowisk chmurowych z wykorzystaniem Defender for Cloud.
- Uczestnicy nauczą się monitorować zgodność i wdrażać środki zaradcze.

Moduł 11: Kontrole zgodności i raportowanie

- Tworzenie raportów zgodności, analiza wyników i przygotowanie organizacji do audytów.

Moduł 12: Tworzenie polityk bezpieczeństwa i ich egzekwowanie

- Projektowanie i wdrażanie polityk bezpieczeństwa w oparciu o najlepsze praktyki.
- Uczestnicy stworzą własne polityki i przetestują ich skuteczność.

Moduł 13: Przegląd innych rodzajów Defenderów

- Przegląd innych rodzajów Defenderów typu Defender for Cloud Apps, Defender for Servers itd.

Moduł 14: Podsumowanie, Q&A, certyfikacja i dalsze kroki

- Omówienie kluczowych wniosków, sesja pytań i odpowiedzi, wręczenie certyfikatów oraz wskazanie dalszych ścieżek rozwoju.

Zapisz się na szkolenie: szkolenia@zalnet.pl

https://zalnet.pl/edu/blue-team-w-praktyce-microsoft-intune-i-defender/