

Szkolenie: Microsoft

SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Microsoft
Partner

Cel szkolenia:

Wdrażanie środowiska usługi Microsoft Defender for Endpoint w celu zarządzania urządzeniami, przeprowadzania dochodzeń na punktach końcowych, zarządzania incydentami w usłudze Defender XDR oraz korzystania z zaawansowanego wyszukiwania zagrożeń za pomocą języka Kusto Query Language (KQL) w celu wykrywania unikalnych zagrożeń.

Profil odbiorców:

Analitik ds. zabezpieczeń firmy Microsoft współpracuje z uczestnikami projektu w organizacji w celu zabezpieczenia systemów informatycznych dla organizacji. Ich celem jest zmniejszenie ryzyka organizacyjnego poprzez szybkie korygowanie aktywnych ataków w środowisku, doradzanie w zakresie ulepszeń praktyk ochrony przed zagrożeniami i odwoływania się do naruszeń zasad organizacyjnych odpowiednim uczestnikom projektu.

Umiejętności zdobyte po ukończeniu:

- Obrona przed cyberzagrożeniami za pomocą usługi Microsoft Defender XDR

Plan szkolenia:

- Obrona przed cyberzagrożeniami za pomocą usługi Microsoft Defender XDR
 - Moduł 1: Łagodzenie skutków incydentów przy użyciu usługi Microsoft Defender
 - Moduł 2: Wdrażanie środowiska usługi Microsoft Defender for Endpoint
 - Moduł 3: Konfigurowanie alertów i wykrywania w usłudze Microsoft Defender for Endpoint
 - Moduł 4: Konfigurowanie automatyzacji i zarządzanie nią za pomocą usługi Microsoft Defender for Endpoint
 - Moduł 5: Przeprowadzanie dochodzeń na urządzeniach w usłudze Microsoft Defender for Endpoint
 - Moduł 6: Ćwiczenia laboratoryjne z obrony przed cyberzagrożeniami za pomocą usługi Microsoft Defender XDR

Wymagania:

- Doświadczenie w korzystaniu z portalu Microsoft Defender
- Podstawowa wiedza o usłudze Microsoft Defender for Endpoint
- Podstawowa wiedza o usłudze Microsoft Sentinel
- Doświadczenie w korzystaniu z języka Kusto Query Language (KQL) w usłudze Microsoft Sentinel

Poziom trudności



Certyfikaty:

Uczestnicy otrzymają certyfikaty podpisane przez Microsoft (ukończenie kursu). Ten kurs nie jest bezpośrednio powiązany z egzaminem certyfikacyjnym Microsoft.

Prowadzący:

Microsoft Certified Trainer (MCT)