MS-500T00-A: Microsoft 365 Security Administration

Bu eğitimde kuruluşunuzun kaynaklarına kullanıcı erişiminin nasıl güvenli hale getirileceğini öğreneceksiniz. Eğitim, kullanıcı parolasının korunmasını, çok faktörlü kimlik doğrulamasını, Azure Kimlik Koruması'nın nasıl etkinleştirileceğini, Azure AD Connect'in nasıl kurulacağını ve kullanılacağını kapsamakta olup Microsoft 365'deki koşullu erişimi de tanıtmaktadır. Microsoft 365 ortamınızı korumaya yardımcı olan tehdit koruma teknolojileri hakkında da bilgi edineceksiniz. Özellikle de tehdit vektörleri ve Microsoft'un tehditleri azaltmaya yönelik güvenlik çözümleri hakkında bilgi edineceksiniz. Secure Score, Exchange Online koruması, Azure Gelişmiş Tehdit Koruması, Windows Defender Gelişmiş Tehdit Koruması ve tehdit yönetimini öğreneceksiniz Eğitimde Microsoft 365 ortamınızı güvenli hale getirmeye yardımcı olan bilgi koruma teknolojileri hakkında da bilgi edineceksiniz. Eğitim, bilgi haklarıyla yönetilen içerik ve mesaj şifrelemenin yanı sıra veri kaybını önleme ve bilgi korumayı destekleyen etiketler, politikalar ve kuralları ele almaktadır. Son olaraksa Microsoft 365'te arşivleme ve saklamanın yanı sıra veri yönetişimi ve içerik aramaları ve araştırmalarının nasıl yürütüleceği hakkında bilgi edineceksiniz. Bu eğitim, veri saklama ilkelerini ve etiketlerini, SharePoint için yerinde kayıt yönetimini, e-posta saklamayı ve eDiscovery araştırmalarını destekleyen içerik aramalarının nasıl gerçekleştirileceğini kapsamaktadır.

Hedefler

- Microsoft 365'de kullanıcı ve grup erişimini yönetme.
- Azure Kimlik Koruma'yı açıklama ve yönetme.
- Azure AD Connect'i planlama ve uygulamaya koyma.
- Senkronize kullanıcı kimliklerini yönetme.
- Koşullu erişimi açıklama ve kullanma.
- Siber saldırı tehdidi vektörlerini açıklama.
- Microsoft 365'e yönelik güvenlik çözümlerini açıklama.
- Güvenlik duruşunuzu değerlendirmek ve iyileştirmek için Microsoft Secure Score'u kullanma.
- Microsoft 365 için çeşitli gelişmiş tehditten koruma servislerini yapılandırma.

- Güvenli mobil cihazları planlama ve kurma.
- Bilgi hakları yönetimini uygulamaya koyma.
- Office 365'de mesajları güvenli hale getirme.
- Veri Kaybını Önleme politikalarını yapılandırma.
- Bulut Uygulama Güvenliğini kurma ve yönetme.
- Cihazlar için Windows bilgi korumayı uygulamaya koyma.
- Veri arşivleme ve saklama sistemini planlama ve kurma.
- eDiscovery araştırması oluşturma ve yönetme.
- GDPR veri sahibi taleplerini yönetme.
- Hassas etiketleri açıklama ve kullanma.

Ön Koşullar

Öğrenciler, bu eğitime başlamadan önce aşağıdaki becerilere sahip olmalıdır:

- Microsoft Azure'un kavramlarını temel düzeyde anlama.
- Windows 10 cihazlar ile deneyim.
- Office 365 ile deneyim.
- Yetkilendirme ve kimlik doğrulamayı temel düzeyde anlama.
- Bilgisayar ağlarını temel düzeyde anlama.
- Mobil cihazların yönetimi konusunda çalışma bilgisi.

Hedef kitle

Microsoft 365 Güvenlik yöneticisi, güvenlik stratejilerini planlamak ve uygulamak ve çözümlerin kuruluşun politikaları ve düzenlemeleriyle uyumlu olmasını sağlamak için Microsoft 365 Kurumsal Yöneticisi, iş paydaşları ve diğer iş yükü

yöneticileriyle işbirliği yapar. Bu rol, Microsoft 365 kurumsal ortamlarının proaktif olarak güvenliğini de sağlar. Sorumlulukları arasında tehditlere yanıt verme, Microsoft 365 ortamı için güvenlik ve uyumluluk çözümlerini uygulama, yönetme ve izleme yer alır. Bu kişiler, olaylara, soruşturmalara ve veri yönetişiminin uygulanmasına yanıt verirler. Microsoft 365 Güvenlik yöneticisi, Microsoft 365 iş yüklerine ve karma ortamlara aşinadır. Bu rol, kimlik koruması, bilgi koruması, tehdit koruması, güvenlik yönetimi ve veri yönetişimi konularında güçlü becerilere ve deneyime sahiptir.

Topics

- User and Group Security
- Identity Synchronization
- Federated Identities
- Access Management
- Security in Microsoft 365
- Advanced Threat Protection
- Threat Intelligence
- Information Protection
- Data Loss Prevention
- Cloud Application Security
- Archiving and Retention
- Data Governance in Microsoft 365
- Managing Search and Investigations