# TEMEL SEVİYE SİBER OLAY YÖNETİMİ VE MÜDAHALE EĞİTİMİ

## 2 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

# İçindekiler

# Eğitim Hakkında

Temel seviye Siber Olay Yönetimi ve Müdahale Eğitimi, katılımcılara bir şirketin veya organizasyonun siber güvenlik ihlallerine veya tehditlere nasıl yanıt verebileceği konusunda gerekli bilgi ve beceriyi kazandırır.

Bu eğitim aşağıdaki konuları genellikle kapsar:

Siber Olay Tanımı:Burada, bir siber olayın ne olduğunu, farklı türlerini ve bu tür olayların bir işletmeye veya organizasyona nasıl etki edebileceğini öğrenir katılımcılar.

Siber Olay Yönetiminin İlkeleri:Bu kısımda, siber olay yönetiminin temel prensiplerini keşfeder ve yanıt planları oluşturma konusunda bilgi edinirler.

Siber Olay Algılama ve İzleme:Katılımcılar, bu bölümde siber olayları belirlemek ve izlemek için gerekli araçlar ve teknikleri incelerler.

Siber Olaylara Yanıt Verme:Prosedürleri, politikaları ve protokolleri araştırarak siber olaylara nasıl müdahale edeceklerini öğrenir katılımcılar.

Olay Sonrası Analiz:Bir olayın etkilerini nasıl analiz edeceklerini ve gelecekteki olayları önlemek veya hafifletmek için ne tür dersler çıkarıp nasıl uygulayacaklarını öğrenirler katılımcılar.

Siber Olayları Önleme Stratejileri: Siber olayları önlemek ve potansiyel riskleri en aza indirgemek için hangi stratejilerin ve araçların kullanılabileceğini öğrenirler.

Sürekli İyileştirme: Bu bölümde, siber olay yönetiminin sürekli bir süreç olduğunu ve sürekli iyileştirme ve adapte olmanın önemini kavrarlar katılımcılar.

Bu eğitimin sonunda, katılımcılar bir siber olayı nasıl tanımlayacaklarını, izleyeceklerini, analiz edeceklerini ve nasıl müdahale edeceklerini öğrenmiş olurlar. İleri seviye eğitimler daha derin ve teknik bilgi sağlar ve belirli araçların veya tekniklerin kullanımına daha çok odaklanır.

# Neler Öğreneceksiniz?

Temel Seviyede Siber Olay Yönetimi ve Müdahale Eğitimi eğitiminde, şunları öğrenebilirsiniz:

- Siber güvenlik kavramları: Siber güvenlik kavramlarını ve terminolojilerini öğreneceksiniz.
- Siber saldırı tanımlama: Siber saldırıların nasıl tanımlanabileceğini ve algılanabileceğini öğreneceksiniz.
- Siber saldırı yönetimi: Siber saldırıların nasıl yönetileceğini ve yanıt verileceğini öğreneceksiniz.
- Siber saldırıların nedenleri: Siber saldırıların nedenlerini ve farklı türlerini öğreneceksiniz.

- Siber saldırıları önleme ve engelleme: Siber saldırıların nasıl önlenebileceğini ve engellebileceğini öğreneceksiniz.
- Siber saldırı sonrası adımlar: Siber saldırı sonrası yapılması gereken adımları öğrenin.
- Veri kaybını önleme: Veri kaybını nasıl önlenebileceğini öğreneceksiniz.
- Siber saldırıların etkilerinin azaltılması: Siber saldırıların etkilerinin nasıl azaltılabileceğini öğreneceksiniz.
- Siber güvenlik ekibi oluşturma: Siber güvenlik ekibi nasıl oluşturulabileceğini öğreneceksiniz.
- İşletme süreçleri güncelleme: İşletme süreçlerinin nasıl güncellenebileceğini öğreneceksiniz.

Bu eğitim, siber güvenliği hakkında temel bilgi ve beceriler kazandırmayı hedefler ve siber saldırılarla başa çıkmak için gerekli olan becerileri kazandırır.

# Ön Koşullar

Temel Seviyede Siber Olay Yönetimi ve Müdahale Eğitimi eğitiminin belirli bir ön koşulu yoktur. Ancak, eğitimi daha verimli hale getirmek için bilgisayar ve internet kullanımının temel seviyede bilinmesi faydalı olabilir. Ayrıca, eğitimi almak isteyen kişinin IT veya siber güvenlik alanında çalışmak istemesi veya ilgisi olması, eğitimin daha anlamlı ve yararlı olmasını sağlayabilir.

# Kimler Katılmalı

Temel Seviyede Siber Olay Yönetimi ve Müdahale Eğitimi eğitimi, siber güvenliği konusunda ilgilenen ve/veya bu alanda çalışan kişiler için uygundur. Aşağıdaki kişiler, bu eğitimden yararlanabilir:

- IT profesyonelleri: IT alanında çalışan kişiler, siber saldırılarla nasıl başa çıkacaklarını ve nasıl önleneceğini öğrenebilir.
- Siber güvenlik uzmanları: Siber güvenlik uzmanları, temel siber güvenlik becerilerini ve yönetim tekniklerini geliştirebilir.
- İşletme yöneticileri: İşletme yöneticileri, işletmelerinin siber güvenliğini nasıl koruyabileceklerini ve siber saldırılarla nasıl başa çıkabileceklerini öğrenebilir.
- Üniversite öğrencileri: Üniversite öğrencileri, siber güvenlik konusunda ilgi duyuyorlar ve bu alanda kariyer yapmak istiyorlar ise bu eğitimden faydalanabilirler.
- İnternet kullanıcıları: İnternet kullanıcıları, siber güvenlik konularına daha fazla özen göstermeyi ve kendilerini ve bilgilerini koruyabilecek becerileri kazanmayı amaçlıyorlarsa bu eğitimden faydalanabilirler.

Bu eğitim, siber güvenliği hakkında bilgi sahibi olmak isteyen ve/veya bu alanda çalışmak isteyen herkes için faydalı olabilir.

# Outline

## 1. Gün: Siber Olayların Tespiti ve İlk Analizi

**Siber Olayların Anlaşılması ve Tespiti**

- Siber güvenlik olaylarının tanımı ve önemi.
- Temel tehdit türleri: Malware, phishing, DDoS saldırıları, iç tehditler.
- Güvenlik ihlallerini tespit etmek için kullanılan temel araçlar ve teknikler.
- Güvenlik duvarları, IDS/IPS sistemleri ve log analizi.

**İlk Yanıt ve Olay İzleme**

- İlk yanıt stratejileri: Etkilenen sistemlerin izolasyonu ve kanıtların korunması.
- Olay kayıtlarının ve logların analizi.
- Temel dijital adliye teknikleri ve araçları.
- Olay izleme ve raporlama süreçleri.

## 2. Gün: Olay Müdahalesi ve Sonrası İşlemler

**Olay Müdahalesi**

- Etkili olay müdahale planlarının oluşturulması.
- Olaya müdahale ekiplerinin rolleri ve sorumlulukları.
- Zararın sınırlandırılması ve sistemlerin yeniden çalışır hale getirilmesi.
- Olay müdahalesinde iletişim ve kriz yönetimi.

**İyileştirme ve Önleme Stratejileri**

- İyileştirme süreçleri: Sistemlerin güvenliğinin yeniden sağlanması.
- İhlalin nedenlerinin analizi ve gelecekteki tehditlere karşı koruma.
- Siber güvenlik farkındalığı ve eğitimi.
- Sürekli iyileştirme için olay sonrası inceleme ve geri bildirim.