SİBER SALDIRI VE SAVUNMAYA GİRİŞ EĞİTİMİ

2 GÜN

Digital Vizyon Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

"Siber Saldırı ve Savunmaya Giriş Eğitimi", katılımcılara siber tehditler ve saldırılar hakkında genel bir anlayış sağlar ve bunlara karşı savunma stratejilerini öğretir. İşte bu eğitimin tipik öğeleri:

- Siber Tehditlerin ve Saldırıların Anlaşılması: Bu bölüm, farklı türdeki siber saldırıları ve tehditleri tanımlar ve genellikle bu saldırıların nasıl gerçekleştirildiğine dair bilgi verir. Virüsler, truva atları, fidye yazılımları ve diğer zararlı yazılımlar bu kategoride yer alır.
- Savunma Stratejileri: Katılımcılar, siber tehditlere ve saldırılara karşı nasıl savunma yapılacağını öğrenir. Güvenlik duvarları, antivirüs yazılımları, yama yönetimi ve diğer koruma teknikleri burada ele alınır.
- Saldırı Tespit ve İzleme: Bu bölümde, katılımcılar bir siber saldırının belirtilerini tanımak ve bunları nasıl izleyeceğini öğrenir. Ayrıca saldırı tespiti ve önleme sistemlerinin (IDS / IPS) kullanımı da bu bölümde ele alınır.
- Olay Yanıtı ve İyileştirme: Katılımcılar, bir siber olaya nasıl yanıt verileceğini ve olay sonrası işletme operasyonlarının nasıl sürdürüleceğini öğrenir.
- Risk Değerlendirmesi ve Yönetimi: Bu bölümde, katılımcılar bir şirketin siber güvenlik risklerini nasıl değerlendireceğini ve yöneteceğini öğrenir.
- Yasal Düzenlemeler ve Uyumluluk: Bu bölüm genellikle siber güvenlikle ilgili yasal düzenlemeleri ve uyumluluk gerekliliklerini anlatır.

Bu temel bilgileri öğrendikten sonra, katılımcılar daha ileri düzey konulara, örneğin sızma testleri ve ileri düzey siber tehdit savunmalarına geçebilir. Siber güvenlik, teknoloji ve siber tehditler sürekli değiştiği için, bu alanda kendinizi sürekli olarak eğitmek ve güncel tutmak önemlidir.

Neler Öğreneceksiniz?

Siber saldırı ve savunma eğitimi alırken, şunları öğrenebilirsiniz:

- Siber saldırıların tanımı ve türleri: Siber saldırıların farklı türlerini ve neden yapıldıklarını öğrenebilirsiniz.
- Ağ güvenliği: Ağ güvenliği konularını, ağları nasıl saldırıya uğrayabileceklerini ve bu saldırıları nasıl önlenebileceğini öğrenebilirsiniz.
- Güvenliği test etme: Ağların güvenliğini test etme yöntemlerini öğrenebilirsiniz.
- Siber suçlar ve suçlu profilleri: Siber suçların türlerini, nasıl yapıldıklarını ve suçlu profillerini öğrenebilirsiniz.
- Siber savunma teknolojileri ve yazılımları: Farklı siber savunma teknolojileri ve yazılımlarını öğrenebilirsiniz.
- Güncel siber güvenlik tehditleri: Güncel siber güvenlik tehditlerini ve bunları nasıl önleyebileceğinizi öğrenebilirsiniz.

Eğitim, teorik olarak verilen konuların yanı sıra, uygulamalı olarak da gerçek dünya senaryolarında çalışmanızı ve öğrendiklerinizi uygulamanızı içerebilir. Böylece, teorik bilgilerinizi pratik uygulamalarla destekleyebilirsiniz.

Ön Koşullar

Siber saldırı ve savunma eğitimi için belirli bir ön koşulu bulunmaz, ancak şu bilgi ve becerilere sahip olmanız eğitimin verimliliğini artırabilir:

- Bilgisayar ve ağ bilgisi: Bilgisayar ve ağlar hakkında temel bilgiye sahip olmanız eğitim sürecini daha verimli hale getirebilir.
- Programlama dilleri: Programlama dilleri hakkında temel bilgiye sahip olmanız, siber saldırı ve savunma tekniklerinin nasıl uygulandığını daha iyi anlamanıza yardımcı olabilir.
- İngilizce okuma ve yazma becerileri: Siber güvenlik alanında yaygın olarak kullanılan bir dil olan İngilizce okuma ve yazma becerilerine sahip olmanız eğitim materyallerinin anlaşılmasını ve uygulamanın daha kolay hale gelmesini sağlayabilir.

Bu ön koşulların hiçbiri zorunlu değildir ve herkesin siber saldırı ve savunma eğitimi almasına izin verilir. Ancak, bu becerilere sahip olmanız eğitim sürecinin daha verimli ve kolay olmasına yardımcı olabilir.

Kimler Katılmalı

Siber saldırı ve savunma eğitimi, şu kişiler katılabilir:

- Ağ güvenliği profesyonelleri: Ağ güvenliği alanında çalışan profesyoneller, eğitim sürecinde öğrendikleri bilgileri pratikte uygulayabilir ve ağlarını daha güvenli hale getirebilirler.
- Bilgi güvenliği yöneticileri: Bilgi güvenliği yöneticileri, eğitim sürecinde öğrendikleri bilgileri şirketlerinin bilgi güvenliği stratejilerini oluşturmada kullanabilirler.
- Sistem ve ağ yöneticileri: Sistem ve ağ yöneticileri, eğitim sürecinde öğrendikleri bilgileri ağlarını ve sistemlerini koruma konusunda kullanabilirler.
- Bilgisayar programcıları ve mühendisleri: Bilgisayar programcıları ve mühendisleri, eğitim sürecinde öğrendikleri bilgileri güvenli yazılımlar tasarımında kullanabilirler.

Siber güvenlik endüstrisinde çalışmak isteyenler: Siber güvenlik endüstrisinde kariyer yapmak isteyen kişiler, eğitim sürecinde öğrendikleri bilgilerle pazarda aranan becerilere sahip olabilirler. Bu kişilerin yanı sıra, herhangi bir bilgi güvenliği konusunda ilgi duyan herkes de siber saldırı ve savunma eğitimine katılabilir.