# CERTIFIED NETWORK DEFENDER (CND) EĞİTİMİ

**5 GÜN**

Digital Vizyon
Akademi

www.digitalvizyon.net

# İçindekiler

# Eğitim Hakkında

Certified Network Defender (CND) Eğitimi, bilgi güvenliği profesyonellerine ağ güvenliği konusunda derinlemesine bilgi ve becerilerin kazandırılmasını amaçlayan özel bir programdır. Bu kapsamlı eğitim, ağ güvenliği tehditlerini anlamanızı, ağ güvenlik önlemlerini uygulamanızı ve ağ güvenlik olaylarını etkin bir şekilde yönetmenizi sağlar. CND eğitimi, bilgi güvenliği konusunda uzmanlaşmak ve ağ güvenliği alanında yetkinlik kazanmak isteyen profesyoneller için tasarlanmıştır. Bu sayede katılımcılar, ağ güvenliği tehditlerini tanıma ve analiz etme becerilerini geliştirir.

CND Eğitimi ayrıca, ağ güvenliği önlemlerini etkin bir şekilde uygulama ve yönetme becerilerini kazandırır. Güvenlik duvarları, saldırı tespit ve önleme sistemleri, sanal özel ağlar (VPN), güvenlik politikaları gibi konular ayrıntılı bir şekilde ele alınır. Bu sayede katılımcılar, ağ güvenliği için en iyi uygulamaları öğrenerek, ağ güvenliği stratejilerini başarılı bir şekilde oluşturabilme yetkinliğini elde eder.

Siber güvenlik uzmanları, genellikle teorik bilgiden öteye geçerek, gerçek dünya uygulamalarında geniş deneyime sahip olmalıdırlar. Bu nedenle, CND (Sertifikalı Ağ Savunma) Eğitiminde, uygulama deneyimleri ve pratik çalışmalar ana odak noktasını oluşturur.

Eğitim boyunca, katılımcılar bir dizi pratik beceri geliştirmek için özel çalışmalara katılırlar. Bu beceriler arasında, katılımcılar güvenlik olaylarını tespit etmeyi, analiz etmeyi ve hızlı bir şekilde yanıt vermeyi öğrenirler. Katılımcılar, karmaşık veya sürekli tehdit durumlarını yönetme yeteneği de dahil olmak üzere, geniş kapsamlı ağ güvenliği becerilerini elde ederler.

Güvenlik olaylarını tespit etmek, genellikle bir ağdaki anormal veya şüpheli aktiviteleri belirlemek anlamına gelir. Bu aktiviteler genellikle saldırıların veya güvenlik ihlallerinin ilk belirtilerini oluşturur.

CND eğitimini başarıyla tamamlayan katılımcılar, EC-Council tarafından verilen CND sertifikasını elde ederler. Certified Network Defender (CND) Eğitimi buradan ulaşabilirsiniz**.**

# Neler Öğreneceksiniz?

Certified Network Defender (C|ND) eğitimi sırasında aşağıdaki konuları öğrenebilirsiniz:

Ağ Güvenlik Temelleri: Ağ güvenliği prensiplerini ve temel kavramları öğrenirsiniz. Ağ güvenlik politikaları, güvenlik katmanları, saldırı türleri ve savunma stratejileri gibi konulara aşina olursunuz.

Ağ Savunma Teknikleri: Ağ güvenliğini sağlamak için kullanılan çeşitli teknikleri ve araçları öğrenirsiniz. Güvenlik duvarları, saldırı tespit ve önleme sistemleri (IDS/IPS), sanal özel ağlar (VPN) gibi güvenlik çözümlerinin nasıl yapılandırılacağını ve yönetileceğini öğrenirsiniz.

Ağ Zafiyet Analizi: Ağda güvenlik açıklarını tespit etmek ve bunları gidermek için kullanılan yöntemleri öğrenirsiniz. Zafiyet taramaları, penetrasyon testleri ve zafiyet yönetimi süreçleri üzerinde çalışarak ağ güvenliğini artırmayı öğrenirsiniz.

Saldırı Tespit ve Olay Yanıtı: Anormal ağ aktivitelerini tespit etmek ve ağ saldırılarını hızlı bir şekilde yanıtlamak için kullanılan yöntemleri öğrenirsiniz. Saldırı tespit sistemlerinin (IDS) kullanımı, günlük kayıtların analizi ve olay yanıtı süreçlerini öğrenirsiniz.

Ağ Trafiği Analizi: Ağ trafiğini analiz etmek ve saldırıları tespit etmek için kullanılan teknikleri öğrenirsiniz. Protokol analizi, paket yakalama ve analiz araçları gibi konular üzerinde çalışarak ağ trafiğini izleme ve değerlendirme becerilerinizi geliştirirsiniz.

Ağ Güvenliği İzleme ve Yönetimi: Ağ güvenliği olaylarını izlemek, güvenlik politikalarını uygulamak ve ağ güvenliği olaylarını yönetmek için kullanılan yöntemleri öğrenirsiniz. Güvenlik bilgi ve olay yönetimi (SIEM) araçlarının kullanımı, log yönetimi ve izleme stratejileri gibi konuları ele alırsınız.

Bu eğitim, ağ güvenliği konusunda bilgi ve becerilerinizi geliştirmenizi sağlar. Ağ güvenliği prensiplerini anlamanız, ağ savunma tekniklerini uygulamanız, ağ zafiyetlerini tespit etmeniz ve saldırıları tespit etmek ve yanıtlamak için gerekli yöntemleri kullanmanız konusunda sizi yetkin hale getirir. C|ND sertifikası, ağ güvenliği konusunda yeteneklerinizi kanıtlar ve işverenler için değerli bir referans oluşturur.

# Ön Koşullar

Certified Network Defender (C|ND) eğitimine katılmak için genellikle özel bir ön koşul bulunmamaktadır. Herhangi biri, ağ güvenliği konusunda ilgi duyan ve bilgi ve becerilerini geliştirmek isteyen herkes C|ND eğitimine katılabilir. Ancak, aşağıdaki ön bilgi ve deneyimler, C|ND eğitiminden maksimum fayda sağlamanıza yardımcı olabilir:

Temel Bilgisayar Bilgisi: Bilgisayar sistemleri, işletim sistemleri ve ağların temel kavramları hakkında bir anlayışa sahip olmanız faydalı olacaktır.

Ağ Temelleri: TCP/IP protokolü, IP adresleme, ağ donanımı ve ağ iletişimi gibi ağ temelleri hakkında bir bilgiye sahip olmanız eğitimi daha iyi anlamanızı sağlayacaktır.

Bilgi Güvenliği Temelleri: Bilgi güvenliği kavramları, saldırı türleri, güvenlik önlemleri ve temel güvenlik kontrolleri gibi bilgi güvenliği alanında bir temel anlayışa sahip olmanız faydalı olacaktır.

Bu ön bilgi ve deneyimler, C|ND eğitimine başlamadan önce size avantaj sağlayabilir, ancak kesin bir ön koşul değildir. Eğitimi sağlayan kuruluşun belirlediği spesifik ön koşulları kontrol etmek önemlidir, çünkü gereksinimler farklı kuruluşlar arasında değişebilir. Eğitim sağlayıcının belirlediği ön koşulları karşıladığınızdan emin olmanız önerilir.

# Kimler Katılmalı

- Certified Network Defender (C|ND) eğitimi, ağ güvenliği konusunda bilgi ve becerilerini geliştirmek isteyen çeşitli profesyoneller için uygundur. Aşağıdaki kişiler C|ND eğitimine katılabilir:

- Ağ Güvenliği Uzmanları: Ağ güvenliği alanında çalışan uzmanlar, mevcut bilgi ve becerilerini geliştirmek ve güncel ağ güvenliği tehditlerine karşı daha etkin savunmalar oluşturmak için C|ND eğitimine katılabilirler.
- Sistem ve Ağ Yöneticileri: Ağ ve sistem yöneticileri, organizasyonlarının ağ güvenliğinden sorumlu olan profesyonellerdir. C|ND eğitimi, onlara ağ güvenliği konularında daha derin bir anlayış sağlar ve saldırıları tespit etme ve önleme yeteneklerini artırır.
- Bilgi Güvenliği Analistleri: Bilgi güvenliği analistleri, ağ güvenliği tehditlerini izlemek, analiz etmek ve raporlamakla görevlidir. C|ND eğitimi, analiz becerilerini geliştirmelerine ve ağ güvenliği olaylarını daha etkili bir şekilde yönetmelerine yardımcı olur.
- IT Yöneticileri: IT yöneticileri, organizasyonun ağ altyapısının güvenliğini sağlamak ve riskleri azaltmakla sorumludur. C|ND eğitimi, IT yöneticilerine ağ güvenliği konularında daha fazla bilgi ve beceri kazandırarak daha iyi bir ağ güvenlik stratejisi oluşturmalarına yardımcı olur.
- Network ve Security Mühendisleri: Ağ ve güvenlik mühendisleri, ağ altyapısının tasarımı, yapılandırılması ve güvenliği ile ilgilenirler. C|ND eğitimi, mühendislerin ağ güvenliği konularında derinlemesine bilgi ve beceriler kazanmalarını sağlar.
- Bu, C|ND eğitimine kimlerin katılması gerektiği konusunda genel bir kılavuzdur. Ancak, herhangi biri ağ güvenliği konusunda ilgi ve motivasyona sahipse, bu eğitime katılarak bilgi ve becerilerini geliştirebilirler. Ağ güvenliği alanında çalışan veya çalışmak isteyen herkes, C|ND eğitimine katılabilir ve ağ güvenliği konusundaki yeteneklerini güçlendirebilir.

# Outline

Module 01: Network Attacks and Defense Strategies

Module 02: Administrative Network Security

Module 03: Technical Network Security

Module 04: Network Perimeter Security

Module 05: Endpoint Security-Windows Systems

Module 06: Endpoint Security-Linux Systems

Module 07: Endpoint Security- Mobile Devices

Module 08: Endpoint Security-IoT Devices

Module 09: Administrative Application Security

Module 10: Data Security

Module 11: Enterprise Virtual Network Security

Module 12: Enterprise Cloud Network Security

Module 13: Enterprise Wireless Network Security

Module 14: Network Traffic Monitoring and Analysis

Module 15: Network Logs Monitoring and Analysis

Module 16: Incident Response and Forensic Investigation

Module 17: Business Continuity and Disaster Recovery

Module 18: Risk Anticipation with Risk Management

Module 19: Threat Assessment with Attack Surface Analysis

Module 20: Threat Prediction with Cyber Threat Intelligence