CERTIFIED INCIDENT HANDLER (ECIH) EĞİTİMİ

5 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında

Certified Incident Handler (E|CIH) eğitimi, siber güvenlik endüstrisinde aktif olan veya bu alanda kariyer yapmak isteyen profesyoneller için mükemmel bir seçimdir. Özellikle olay müdahale süreçleri ve bu süreçlerde etkili yöntemlerin kullanımına odaklanır. E|CIH eğitimi, kapsamlı bir yaklaşımla olaylara müdahale süreçlerini ve tekniklerini anlatır, böylece katılımcılar güvenlik olaylarını tespit etme, analiz etme, yanıtlama ve sonrasında iyileştirme becerilerini geliştirirler.

Olay Müdahalesi Temelleri bölümünde, olay müdahalesinin temel kavramları ve yöntemleri hakkında ayrıntılı bilgi veriyoruz. Katılımcılar, olay müdahalesinin önemini, rolleri ve temel süreç adımlarını öğrenirler. Ayrıca, izleme ve yanıt stratejileri ile olay müdahalesi sürecinin etkili bir şekilde nasıl yapılandırılacağı üzerinde duruyoruz. Bu aşamada, iyi organize edilmiş bir olay müdahalesi ekibinin, herhangi bir güvenlik olayına hızlı ve etkili bir şekilde nasıl yanıt verebileceği üzerinde duruyoruz.

Olay Tespiti ve Yanıt Verme kısmında, güvenlik olaylarını tespit etme ve analiz etme yöntemlerine odaklanıyoruz. Acil durum yanıt planlarının nasıl hazırlanacağı ve uygulanacağı, olaylara hızlı ve etkili bir şekilde nasıl yanıt verileceği gibi konular ele alınır. Simülasyonlar ve gerçek hayat örnekleri sayesinde, katılımcılar kritik düşünme ve hızlı karar verme becerilerini keskinleştirir.

Olay İnceleme ve Analiz bölümü, olayların ayrıntılı olarak incelenmesine ve analizine odaklanır. Burada, katılımcılar olay yerinde veri toplama, olayların kronolojik sırasını belirleme ve saldırganın eylemlerini ve motivasyonlarını anlama gibi konularda bilgi sahibi olurlar. Bu, daha sonra olayların kaynağını belirlemek ve güvenlik açıklarını gidermek için önemlidir.

Sistem ve Ağ İzleme bölümünde, katılımcılar log analizi, ağ trafiği izleme, saldırı tespiti sistemleri gibi araçları ve teknikleri kullanarak olay izlemeyi ve tehdit tespitini öğrenirler. Bu beceriler, bir organizasyonun güvenlik duruşunu güçlendirmek ve gelecekteki tehditlere karşı daha hazırlıklı olmak için kritik öneme sahiptir.

Olay Dizisi Yönetimi ve Raporlama bölümü, olayların etkili bir şekilde yönetilmesini, takip edilmesini ve raporlanmasını kapsar. Bu aşamada, katılımcılar olay kaydı, sınıflandırma, takip, ve raporlama için kullanılan en iyi uygulamaları ve araçları öğrenirler.

Certified Incident Handler (E|CIH) eğitimi, bir bütün olarak olay müdahale süreçlerinin kapsamlı bir anlayışını sağlayarak, katılımcılara, güvenlik olaylarına karşı daha proaktif ve etkili bir savunma geliştirmek için gerekli araçları ve bilgiyi sunar. E|CIH sertifikası, katılımcıların bu alanda derinlemesine bilgi ve uygulamalı becerilere sahip olduğunu, ve olay müdahalesi süreçlerinde başarılı bir şekilde çalışabileceklerini kanıtlar.

Neler Öğreneceksiniz?

Certified Incident Handler (E|CIH) eğitimi sırasında aşağıdaki konuları öğrenebilirsiniz:

- Olay Müdahalesi Temelleri: Olay müdahalesi sürecinin temel kavramlarını ve prensiplerini öğrenirsiniz. Olay müdahalesi rol ve sorumlulukları, olay tespiti, bildirim süreci, acil durum planlaması gibi konuları kapsar.
- Olay Tespiti ve Analizi: Olayları tespit etme ve analiz etme yöntemlerini öğrenirsiniz. Olay belirtilerini tanıma, olayları sınıflandırma, olaylara yanıt verme ve sorunları analiz etme becerilerinizi geliştirirsiniz.
- Olay Yanıtı ve Müdahale: Olaylara hızlı ve etkili bir şekilde yanıt verme stratejilerini öğrenirsiniz. Olayları kontrol altına alma, zararları azaltma, saldırıları durdurma ve sistemleri yeniden yapılandırma gibi müdahale süreçlerini uygulama becerilerinizi geliştirirsiniz.
- Olay İnceleme ve Delil Toplama: Olayları ayrıntılı bir şekilde inceleme ve delil toplama yöntemlerini öğrenirsiniz. Olayların kökenini belirleme, saldırı yöntemlerini analiz etme, delil toplama süreçlerini uygulama becerilerinizi geliştirirsiniz.
- Olay Raporlama ve İyileştirme: Olayların raporlanması, olay raporlarının hazırlanması ve olaylardan elde edilen dersleri kullanarak güvenlik önlemlerini iyileştirme süreçlerini öğrenirsiniz. Raporlama becerilerinizi geliştirerek yöneticilere ve ilgili paydaşlara etkili bir şekilde olayları iletebilirsiniz.

E|CIH eğitimi, güvenlik olaylarına etkin bir şekilde yanıt verme yeteneklerinizi geliştirmenizi sağlar. Olayları tespit etme, analiz etme, yanıtlama, delil toplama ve raporlama konularında derinlemesine bilgi ve beceriler kazanarak güvenlik olaylarına müdahale edebilir ve organizasyonunuzun güvenlik durumunu iyileştirebilirsiniz.

Ön Koşullar

Certified Incident Handler (E|CIH) eğitimine katılmadan önce belirli bir ön koşul bulunmamaktadır. Bununla birlikte, aşağıdaki bilgi ve deneyimlere sahip olmanız, eğitimi daha iyi anlamanıza yardımcı olabilir:

- Bilgi Güvenliği Temelleri: Bilgi güvenliği konusunda temel bir anlayışa sahip olmanız önerilir. Güvenlik prensipleri, güvenlik tehditleri ve güvenlik kontrolleri hakkında bilgi sahibi olmak, eğitimi daha verimli hale getirebilir.
- Ağ ve Sistem Güvenliği: Ağ ve sistem güvenliği konularında bir temel bilgiye sahip olmanız faydalı olacaktır. Ağ yapılandırması, ağ protokolleri, güvenlik duvarları, IDS/IPS gibi temel ağ güvenliği kavramlarına aşina olmak, olay müdahalesi süreçlerini anlamanıza yardımcı olabilir.
- Olay Müdahalesi İlgili Deneyim: Önceki olay müdahale deneyimine sahip olmak, eğitimi daha verimli hale getirebilir. Olay müdahalesi süreçlerini, olay tespiti ve analizi, olay yanıtı ve raporlama gibi konuları önceden tecrübe etmiş olmanız, derinlemesine anlamaya ve uygulamaya daha hazır olmanızı sağlar.

Bu ön bilgi ve deneyimler, E|CIH eğitimine katılmadan 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 Incident Handler (E|CIH) eğitimi aşağıdaki profesyonel gruplar için uygundur:

- Bilgi Güvenliği Uzmanları: Bilgi güvenliği alanında çalışan profesyoneller, olay müdahalesi süreçlerini anlamak, güvenlik olaylarını etkili bir şekilde yönetmek ve organizasyonun güvenlik durumunu iyileştirmek için E|CIH eğitimine katılabilirler.
- Güvenlik Operasyon Merkezi (SOC) Personeli: SOC ekiplerinde çalışanlar, güvenlik olaylarını tespit etme, analiz etme, yanıtlama ve raporlama konularında bilgi ve becerilerini geliştirmek için E|CIH eğitimine katılabilirler. Bu eğitim, SOC operasyonlarında etkin bir şekilde çalışmalarına yardımcı olabilir.
- Olay Yanıtı Ekipleri: Olay yanıtı ekipleri, organizasyon içinde güvenlik olaylarına hızlı ve etkili bir şekilde yanıt vermekle görevlidir. E|CIH eğitimi, bu ekiplerin olayları yönetme ve olay müdahalesi süreçlerini uygulama becerilerini geliştirmelerine yardımcı olur.
- Sistem ve Ağ Yöneticileri: Sistem ve ağ yöneticileri, organizasyonun ağ altyapısının güvenliğini sağlamak ve olayları etkili bir şekilde yönetmekle sorumludur. E|CIH eğitimi, bu yöneticilere güvenlik olaylarını tespit etme, analiz etme ve yanıtlama konularında bilgi ve beceri kazandırır.
- Güvenlik Danışmanları ve Denetçiler: Güvenlik danışmanları ve denetçiler, müşterilere olay müdahale ve güvenlik olayları yönetimi konularında rehberlik etmek isteyebilirler. E|CIH eğitimi, danışmanlık ve denetim süreçlerinde güvenlik olaylarına etkin bir şekilde yanıt verme yeteneklerini geliştirmek için uygundur.

Yukarıda belirtilen gruplar, E|CIH eğitimine katılmak için uygun olabilecek örneklerdir. Ancak, herhangi biri, olay müdahalesi süreçleri ve güvenlik olaylarına etkili bir şekilde yanıt verme konularında ilgi ve motivasyona sahipse, bu eğitime katılarak bilgi ve becerilerini geliştirebilirler. Olay müdahalesi ve güvenlik olayları yönetimi alanında çalışmak isteyen veya mevcut bilgi ve becerilerini güçlendirmek isteyen herkes, E|CIH eğitimine katılabilir.

Outline

Module 01: Introduction to Incident Handling and Response

Module 02: Incident Handling and Response Process

Module 03: Forensic Readiness and First Response

Module 04: Handling and Responding to Malware Incidents

Module 05: Handling and Responding to Email Security Incidents

Module 06: Handling and Responding to Network Security Incidents

Module 07: Handling and Responding to Web Application Security Incidents

Module 08: Handling and Responding to Cloud Security Incidents

Module 09: Handling and Responding to Insider Threats