SİBER OLAY VEYA BİLGİ GÜVENLİĞİ İHLAL OLAYI TESPİTİ VE RAPORLAMASI EĞİTİMİ

2 GÜN

Digital Vizyon Akademi

www.digitalvizyon.net

Eğitim Hakkında

Günümüzün dijital çağında, siber güvenlik, işletmelerin ve bireylerin en çok önem verdiği alanlardan biri haline gelmiştir. Özellikle siber olayların ve bilgi güvenliği ihlallerinin doğru bir şekilde tespit edilmesi, hızlı ve etkili müdahale edilmesi önem taşır. Bununla birlikte, bu olayların detaylı bir şekilde raporlanması, işletmelerin potansiyel zararları en aza indirmesi gerekir. Ayrıca, gelecekteki benzer tehditleri önlemesi açısından büyük önem taşır. Bunun yanı sıra, "Siber Olay veya Bilgi Güvenliği İhlal Olayı Tespiti ve Raporlaması Eğitimi", katılımcılara bu konuda kapsamlı bir rehberlik sunmaktadır.

Eğitim programımız, siber güvenlik tehditlerinin ve zafiyetlerinin nasıl tespit edileceği üzerinde durulmaktadır. Bununla birlikte, bu tehditlere nasıl müdahale edileceğini ele alır. Ayrıca, müdahale sonrasında yaşanan olayların nasıl raporlanacağı üzerine yoğunlaşmaktadır. Katılımcılar, gerçekçi olay simülasyonlarıyla desteklenen interaktif bir ortamda, teorik bilgilerini uygulamalı olarak pekiştirme şansı bulacaklar. Bu simülasyonlar, katılımcılara gerçek hayatta karşılaşabilecekleri siber güvenlik senaryoları üzerinde çalışma imkânı tanımaktadır. Ayrıca, alınacak önlemler ve yapılacak müdahaleler konusunda derinlemesine tecrübe kazandırmaktadır.

"Siber Olay veya Bilgi Güvenliği İhlal Olayı Tespiti ve Raporlaması Eğitimi", sadece teorik bir eğitim değildir. Katılımcılarına siber güvenlik dünyasında karşılaşabilecekleri gerçek senaryolara karşı hazırlıklı olma becerisi kazandırmayı amaçlamaktadır. Eğitimimiz, siber güvenlik alanında kariyer yapmayı hedefleyen profesyoneller içindir. Bunun yanı sıra, IT uzmanları, kurumsal güvenlik yöneticileri ve siber güvenlikle ilgilenen herkes için idealdir. Eğitimin sonunda katılımcılar, siber güvenlik ihlallerini profesyonelce tespit etme konusunda gelişmektedir. Bununla birlikte, etkili müdahale etmeyi öğretir. Bununla birlikte, olayları şirket içinde veya ilgili otoritelere doğru bir şekilde raporlama konusunda yetkinlik kazanmaktadır.

Neler Öğreneceksiniz

- Siber Güvenlik Tehditleri ve Zafiyetleri: Tehdit türlerini, saldırı vektörlerini ve bilgi güvenliği zafiyetlerini tanıma.
- Olay Tespiti: Güvenlik ihlallerini ve siber olayları tespit etme teknikleri.
- Olaylara Müdahale: Etkili bir siber olay müdahale sürecinin nasıl yönetileceği.
- Olay Sonrası İnceleme ve Analiz: İhlallerin kök nedenlerinin analizi ve zararın boyutunun değerlendirilmesi.
- Raporlama ve İletişim: İhlal olaylarının raporlanması ve ilgili taraflara etkili bir şekilde iletişimi.
- Kurtarma ve Yeniden Kurma: Sistemlerin güvenli bir şekilde yeniden kurulması ve iş sürekliliğinin sağlanması.
- Yasal Uyum ve Standartlar: GDPR, HIPAA gibi uyum gereksinimleri ve bunlara uyum sağlama yolları.

Kimler Katılmalı

- Bilgi güvenliği profesyonelleri, siber güvenlik uzmanları ve analistleri.
- IT yöneticileri ve sistem yöneticileri.
- Risk yönetimi ve uyum ile ilgilenen profesyoneller.

- Kurumsal güvenlik planlaması yapan stratejistler.
- İç denetçiler ve siber güvenlik eğitimi almak isteyen diğer ilgili çalışanlar.

Ön Koşullar

- Temel bilgisayar ve internet teknolojileri bilgisi.
- Temel düzeyde bilgi güvenliği veya IT deneyimi.

Eğitim İçeriği

Modül 1: Siber Güvenlik Olaylarının Anlaşılması

- **Siber Güvenlik Olayı ve Güvenlik İhlali Arasındaki Farklar**: Bu bölümde, olay ve ihlal terimlerinin tanımları, aralarındaki farklar ve her ikisinin organizasyona etkileri anlatılacaktır.
- **Temel Terminoloji ve Konseptler**: Siber güvenlikle ilgili temel terimler, tehdit, zafiyet, risk gibi kavramların açıklamaları yapılacak.
- **Olay Türlerine Genel Bakış**: Malware, ransomware, phishing, DDoS saldırıları ve iç tehditler gibi sık karşılaşılan siber olay türleri detaylandırılacak.

Modül 2: İhlal Tespiti

- **İhlal Tespit Sistemleri ve Kullanımı**: Intrusion Detection Systems (IDS) ve Intrusion Prevention Systems (IPS) gibi sistemlerin kurulumu, konfigürasyonu ve yönetimi üzerine eğitim verilecek.
- **Anomali ve İmza Tabanlı Tespit Teknikleri**: Anomaliye dayalı tespit ve imza bazlı tespit metodolojileri, avantajları ve sınırlılıkları anlatılacak.
- **Günlük Kayıtları ve Olay İzlemeleri ile Tespit**: Log yönetimi, önemli log bilgilerinin nasıl analiz edileceği ve olay izleme teknikleri öğretilecek.

Modül 3: Olaya Yanıt Verme

- **İlk Yanıt Prosedürleri**: Bir güvenlik ihlali tespit edildiğinde izlenecek ilk adımlar, acil durum ekiplerinin aktivasyonu.
- **Olayın Kapsamını Belirleme**: Olayın etkilediği sistemlerin ve verilerin hızlı bir şekilde belirlenmesi, olayın boyutunun anlaşılması.
- **Etkilenen Sistemlerin İzolasyonu ve Zararın Minimizasyonu**: İhlalin yayılmasını önlemek için sistemlerin izole edilmesi, zararın minimize edilmesi için yapılan işlemler.

Modül 4: Olay Analizi

- **Olay Analizi Teknikleri**: Etkili bir olay analizi için kullanılan metodolojiler ve araçlar.
- **Root Cause Analizi**: Güvenlik ihlalinin temel sebeplerinin derinlemesine incelenmesi.
- **Olay Sırasında ve Sonrasında Toplanan Verilerin Analizi**: Olay sırasında toplanan verilerin ve günlüklerin detaylı analizi.

Modül 5: Raporlama ve İletişim

- **Olay Raporlama Formatları ve İçeriği**: Standart olay raporlama formatları, raporlamanın önemli unsurları.
- **İlgili Taraflarla Etkili İletişim**: İç ve dış paydaşlarla iletişim stratejileri, kriz iletişimi.
- **Yasal Gereklilikler ve Uyumluluk**: İlgili yasal gereklilikler, raporlamanın yasal zorunlulukları.

Modül 6: Olay Sonrası İnceleme ve Önleyici Önlemler

- **Olay Sonrası İnceleme Süreçleri**: İhlal olayının ardından yapılan detaylı incelemeler, süreçlerin gözden geçirilmesi.
- **Ders Alınanlar ve İyileştirme Planları**: İhlalden çıkarılan dersler, iyileştirme ve geliştirme için yapılan planlamalar.
- **Önleyici Güvenlik Önlemleri ve Politika Geliştirmeleri**: Güvenlik ihlallerini önlemek için alınabilecek proaktif önlemler ve organizasyonel güvenlik politikalarının geliştirilmesi. Bu kısımda, daha güçlü güvenlik mimarilerinin oluşturulması, eğitim programlarının iyileştirilmesi ve teknolojik yatırımların artırılması gibi stratejiler üzerinde durulacak.

Öğrenme Yöntemleri

- **Uygulamalı Laboratuvar Çalışmaları**: Katılımcılar, sanal laboratuvar ortamında gerçek siber güvenlik olaylarına müdahale edecekler.
- **Gerçek Olay Senaryoları Üzerinden Simülasyonlar**: Gerçek dünyadan alınmış siber olay senaryoları kullanılarak, katılımcıların olaya yanıt verme ve sorun çözme becerileri pekiştirilecek.
- **Grup Çalışmaları ve Tartışmalar**: Katılımcılar, farklı senaryolar üzerinde gruplar halinde çalışacak ve çeşitli çözüm yollarını tartışacaklar.

Eğitmen Profili

- **Uzman Eğitmenler**: Eğitim, siber güvenlik alanında en az on yıl tecrübeye sahip, akademik ve sektörel bilgilerle donanmış eğitmenler tarafından verilecektir. Bu eğitmenler, katılımcıların siber güvenlik konusundaki bilgi ve becerilerini geliştirmelerine yardımcı olacak pratik ve teorik bilgileri aktaracaklardır.

Eğitim Sonunda Katılımcılara Sağlanacaklar

- **Katılım Sertifikası**: Eğitim sonunda tüm katılımcılara 'Siber Olay veya Bilgi Güvenliği İhlal Olayı Tespiti ve Raporlaması' alanında bir katılım sertifikası verilecek.
- **Eğitim Materyalleri**: Eğitim boyunca kullanılan tüm materyaller, katılımcılara dijital formatlarda sunulacak.