

Dijital dünyada işletmelerin karşı karşıya kaldığı siber tehditler giderek daha karmaşık hale geliyor. Bu tehditlerle başa çıkabilmek ve organizasyonel güvenliği sağlam bir temele oturtabilmek için üst düzey yöneticilerin ve birim yöneticilerinin siber güvenlik konusunda derinlemesine bilgiye sahip olmaları kritik bir öneme sahiptir. Bu eğitim, katılımcıların iş dünyasındaki siber güvenlik stratejileri hakkında bilgi edinmelerini, güvenlik risklerini yönetmelerini ve bu tehditlere karşı güçlü savunma sistemleri kurmalarını sağlamayı hedefliyor.

KURUMSAL ÖZEL EĞİTİM

Bu konuyu istediğiniz gibi özelleştirebilirsiniz. Kullandığınız teknolojiye özel uygulamalar ile anlatılmasını, projenize uygun içerik haline getirilmesini ...



- **Siber Güvenlik Yönetimi:** Tepe yöneticilerinin organizasyonel güvenliği nasıl güçlendirebileceği ve risk yönetimi süreçlerini nasıl optimize edebileceği konusunda derinlemesine bilgi.
- **Risk ve Tehdit Yönetimi:** Siber tehditleri öngörme, riskleri analiz etme ve etkili bir risk yönetimi planı oluşturma becerileri.
- **Kurumsal Güvenlik Stratejisi Geliştirme:** Yöneticilerin, iş süreçleriyle uyumlu, sürdürülebilir bir güvenlik stratejisi oluşturma yolları.
- **Etik ve Yasal Düzenlemeler:** Siber güvenlik ve veri gizliliği konusunda en son yasal düzenlemeler ve etik kurallar hakkında bilgi.

Bu eğitim, üst düzey yöneticilere ve karar vericilere, siber güvenliğin iş stratejileri ile entegrasyonunu sağlamaları için gerekli bilgileri sunmayı amaçlamaktadır. Katılımcılar, organizasyonlarında güvenlik kültürünü benimsemek, risk yönetimi süreçlerini iyileştirmek ve siber tehditlere karşı proaktif stratejiler geliştirmek için gerekli becerileri kazanacaklardır. Eğitim, siber güvenlikteki en son trendler ve teknolojiler hakkında derinlemesine bilgi sağlayarak, yöneticilerin güvenlik politikalarını etkin bir şekilde oluşturmaya ve liderlik etmesine olanak tanıyacaktır. Ayrıca, organizasyonel güvenliği güçlendirecek ve risklere karşı etkili bir savunma stratejisi oluşturulmasına yardımcı olacak pratik yöntemler sunulacaktır.



EĞİTİM İÇERİĞİ

SİBER GÜVENLİK VE KURUMSAL

HAZIRLIK

- Siber Tehditlerin Tanımlanması ve İş Dünyasına Etkisi: Günümüzde hızla gelişen siber tehditlerin iş dünyasında yaratabileceği tehlikeler, saldırı türleri ve bunların potansiyel etkileri. Örneğin, veritabanı saldırıları veya fidye yazılımları gibi tehditler, şirketlerin itibarını ve finansal durumunu ciddi şekilde etkileyebilir.
- Siber Güvenlik Stratejileri ve Kurumsal Uyum: Kurumların güvenlik stratejileri geliştirme ve bu stratejileri kurum kültürüne entegre etme süreci. Ayrıca, bu stratejilerin yasal düzenlemelere uyumlu olmasının önemi vurgulanır.
- Yönetici Perspektifinden Risk Değerlendirmesi: Kurumların siber güvenlik tehditlerine karşı riskleri nasıl değerlendirebileceği ve bu süreçte yöneticilerin alması gereken kararlar. Yöneticilerin bilgi kaybı veya itibar kaybı gibi potansiyel tazminatlarla karşılaşmamak için alacağı önlemler.
- Veri Güvenliği ve Gizliliği: Kurumların KVKK'ya uyumlu veri güvenliği politikaları oluşturması, gizliliğin sağlanması ve verilerin korunması için alınacak önlemler.

İLERİ SEVİYE GÜVENLİK

TEKNOLOJİLERİ VE ALTYAPI

- İleri Seviye Güvenlik Duvarları ve Saldırı Tespit Sistemleri: Gelişmiş ağ güvenlik sistemleri ve saldırı tespit/önleme sistemleri, kurumların altyapı güvenliğini sağlamada kritik öneme sahiptir. Ayrıca, bu sistemler, şirketlerin dış saldırılara karşı etkili korunmasına yardımcı olur.

- DDoS Saldırıları ve Önleme Stratejileri: Dağıtılmış hizmet dışı bırakma saldırıları (DDoS) gibi siber saldırılar, ağır çalışmasını engelleyebilir ve şirketin hizmetlerini kesintiye uğratabilir. Bu tür saldırılara karşı alacağı önlemler, itibar kaybını ve finansal zararı önleyebilir.
- Zararlı Yazılım Tespiti ve Yanıt Stratejileri: Zararlı yazılımların tespiti ve bu yazılımlara karşı geliştirilen hızlı müdahale stratejileri. Bu, potansiyel veri kayıplarını ve bilgi sızıntılarını engellemek için kritik öneme sahiptir.
- Güvenli Altyapı ve Bulut Bilişim: Bulut altyapıları, kurumların veri güvenliğini sağlamada önemli bir rol oynar. Ancak, KVKK'ya uygunluk ve verilerin bulut ortamlarında güvenli bir şekilde saklanması, şirketlerin hukuki sorumluluklarını yerine getirmeleri için gereklidir.

SİBER GÜVENLİKTE LİDERLİK VE DEĞİŞİM YÖNETİMİ

- Siber Güvenlik Liderliği: Yöneticilerin siber güvenlik stratejileri oluşturma ve uygulama konusunda liderlik yapabilme becerileri. Bu liderlik, organizasyonun güvenliğini sağlamak ve itibar kaybının önüne geçmek için kritik öneme sahiptir.
- Kurumsal Kültür ve Siber Güvenlik Uyum: Kurum kültürünün siber güvenlik stratejileriyle uyumlu hale getirilmesi. Çalışanların güvenlik bilincinin artırılması ve bu kültürün şirketin her katmanında benimsenmesi, büyük çaplı veri sızıntıları ve güvenlik ihlallerinin önüne geçebilir.
- Risk Yönetimi ve Olay Müdahale Protokolleri: Bir siber güvenlik olayı sonrası alınacak acil önlemler, kriz yönetimi ve olay müdahale süreçleri. Etkin olay müdahalesi, itibar kaybı ve yasal tazminatların önüne geçilmesini sağlayabilir.

- Etik ve Hukuki Perspektif: Yasal sorumluluklar ve etik kuralların siber güvenlik süreçlerine entegrasyonu. KVKK gibi yasal düzenlemelere uyumsuzluk, firmaların ciddi tazminatlarla karşılaşmasına yol açabilir.

STRATEJİK KARAR VERME VE YZ UYGULAMALARI İLE GÜVENLİK İNOVASYONU

- Yapay Zeka ve Güvenlik İnovasyonu: Yapay zeka temelli güvenlik çözümleri, proaktif tehdit tespiti ve önleme stratejileri. Yapay zeka, siber saldırıları hızlı bir şekilde tanıma ve buna karşılık verme yeteneği sunarak büyük çaplı veri kayıplarının ve itibar zararlarının önüne geçebilir.
- Siber Güvenlik Projelerinde KPI ve ROI Yönetimi: Siber güvenlik projelerinin başarısını ölçmek için KPI'lar ve ROI hesaplamaları. Bu, şirketlerin güvenlik yatırımlarının etkinliğini değerlendirmelerine ve uzun vadede güvenlik risklerini minimize etmelerine yardımcı olur.
- Sektörel Uygulamalar ve Gelecek Trendleri: Farklı sektörlerdeki siber güvenlik trendleri ve bu sektöre özgü tehditlere karşı alınması gereken önlemler. Bu, sektörel düzeyde güvenlik stratejilerinin nasıl şekillendirileceğini ve organizasyonların gelecekteki tehditlere nasıl adaptasyon sağlayacağını gösterir.
- Siber Güvenlik Geleceği: Gelecekteki siber tehditler, yenilikçi güvenlik çözümleri ve stratejik kararlar üzerine yapılan derinlemesine tartışmalar. Firmaların gelecekteki güvenlik risklerine karşı hazırlıklı olmaları, itibar kaybını ve yüksek tazminatları önleyebilir.



EĞİTİM SÜRESİ

- 1 Gün
- Ders Süresi: 50 dakika
- Eğitim Saati: 10:00 - 17:00

Eğitim formatında eğitimler 50 dakika + 10 dakika moladır. 12:00-13:00 saatleri arasında 1 saat yemek arasındaki verilir. Günde toplam 6 saat eğitim verilir. 1 günlük formatta 6 saat eğitim verilmektedir.

Eğitimler uzaktan eğitim formatında tasarlanmıştır. Her eğitim için teams linkleri gönderilir. Katılımcılar bu linklere girerek eğitimlere katılırlar. Ayrıca farklı remote çalışma araçları da eğitmen tarafından tüm katılımlara sunulur. Katılımcılar bu araçları kullanarak eğitimlere katılırlar.

Eğitim içeriğinde github ve codespace kullanılır. Katılımcılar bu platformlar üzerinden örnek projeler oluşturur ve eğitmenle birlikte eğitimlerde sorulan sorulara ve taleplere uygun içeriğe cevap verir. Katılımcılar bu araçlarla eğitimlerde sorulan sorulara ve taleplere uygun içeriğe cevap verir. Eğitim yapay zeka destekli kendi kendine öğrenme formasyonu ile tasarlanmıştır. Katılımcılar eğitim boyunca kendi kendine öğrenme formasyonu ile eğitimlere katılırlar. Bu eğitim formatı sayesinde tüm katılımcılar gelecek tüm yaşamlarında kendilerini güncellemeye devam edebilecekler ve her türlü sorunun karşısında çözüm bulabilecekleri yeteneklere sahip olacaklardır.

YÖNETİCİLERE YÖNELİK SİBER GÜVENLİK

Eğitim, kurum yöneticilerinin dijital güvenlik konusundaki farkındalıklarını artırmayı ve güvenlik politikalarını etkin bir şekilde yönetebilmelerini sağlamayı amaçlamaktadır. Kurumsal riskleri minimize etmek ve güvenlik kültürünü üst düzeyde oluşturmak için kritik bir araçtır. Çevrim içi veya yüz yüze sunulabilen program, özellikle yönetim kademesindeki çalışanlar için tasarlanmıştır ve güvenlik stratejilerinin nasıl uygulanacağı, izleneceği ve yönlendirileceği konusunda derinlemesine bilgi sunar. Katılımcılar, organizasyonel güvenlik yönetimi, acil durum müdahale planları ve liderlik perspektifinden dijital güvenlik yaklaşımını öğrenirler. Eğitim sonunda katılımcılar, sertifika alarak, güvenli bir dijital ortamın sağlanmasında liderlik rollerini etkili bir şekilde üstlenebilirler. Kurumunuzda güçlü bir siber güvenlik kültürünü en üst seviyeye taşımak istiyorsanız, bu eğitim yöneticiler için kritik bir adım olacaktır.

KATILIMCILARDAN BEKLENTİLERİMİZ

Yöneticilerden, eğitime aktif katılım göstermeleri ve öğrenilen bilgileri günlük iş hayatlarında güvenlik alışkanlıkları olarak uygulamaları beklenmektedir. Eğitimde, şüpheli durumları doğru değerlendirmeleri, güvenlik tehditlerini zamanında ilgili birimlere bildirmeleri ve kurumsal dijital güvenliği artırmak için örnek olmaları önemlidir. Ayrıca, eğitim sonrası geri bildirim vererek sürecin iyileştirilmesine katkı sunmaları beklenmektedir.

EĞİTİM YÖNTEMİ

Eğitim, katılımcıların konuya aktif şekilde dâhil olabileceği etkileşimli bir yapıda planlanmıştır. Teorik bilgilerin sade ve anlaşılır şekilde sunulmasının yanı sıra, gerçek hayattan örnekler ve vaka analizleriyle desteklenerek farkındalık düzeyinin artırılması hedeflenir.

Görsel materyaller, kısa videolar ve senaryo temelli anlatımlar sayesinde dikkat çekici ve akılda kalıcı bir öğrenme ortamı sunulur. Eğitimin sonunda yapılan kısa bilgi testleri ile öğrenilenlerin pekiştirilmesi sağlanır. Eğitim tercihe göre çevrim içi platformlar üzerinden ya da yüz yüze sınıf ortamında uygulanabilir şekilde esnek olarak sunulur.

HEDEF KİTLE

Siber güvenlik, günümüzün dijital dünyasında, sadece IT departmanlarının sorumluluğu değil, tüm kurumsal yöneticilerin kritik bir görevidir. Özellikle, kurumun güvenliğini ön planda tutan, dijital riskleri minimize etmeyi amaçlayan yöneticiler için bu eğitim vazgeçilmezdir. Yöneticiler, şirket stratejileri ve kararlarıyla birlikte siber güvenlik tehditlerine karşı da liderlik etmekle yükümlüdür. Bu eğitim, siber güvenlik risklerini doğru değerlendirebilme, güvenlik politikalarını etkin bir şekilde yönetebilme ve güvenli bir dijital ortam oluşturma konusunda yöneticilere gerekli becerileri kazandırır.

Eğitim, kurumsal güvenliği ön planda tutan, risk yönetimini ciddiyetle ele alan ve çalışanlarına örnek olmayı isteyen yöneticiler için tasarlanmıştır. Eğitimi alarak, yalnızca teknik bilgi değil, aynı zamanda siber güvenlik kültürünü kurumsal düzeyde inşa etme yetkinliği de kazanırsınız.

"

Kurumsal size özel eğitimler hazırlıyoruz. Her eğitim yeni bir heyecan.

Vebende A.Ş.

Kurumsal Terzi Usulü Butik Eğitimler.

Size özel hazırlanan seminer, danışmanlık, eğitim ve hizmetlerimizle yüksek verim elde edin. Paranızı boşa harcamayın. Zaman çok değerli.

Her Eğitim Yeni Bir Heyecan

2000 yılından günümüze devam eden eğitim heyecanı. Uluslararası tecrübe, proje geliştirme deneyimleri, danışmanlıklar ve arge mühendislik deneyimlerimizi ülkemize sunmak için yeni bir konsept tasarladık. Sizi dinliyor, takımınıza uygun özel içerikler ile hazırlanmış eğitimler hazırlıyoruz. Her eğitim özel bir çalışma, içerik üretimi, uygulama örnekleri hazırlıkları, sunumlar hazırlamayı gerektiriyor. Aynı eğitimi yönetim kadrosuna farklı, teknik ve mimar ekiplerinize farklı içerikler ile hazırlıyoruz. Her eğitim yeni bir macera ve heyecan.



Bizimle İletişime Geçin

iletisim@vebende.com

www.vebende.com.tr

İzmir - Türkiye

Kurumsal Eğitimler

www.vebende.com.tr

