MİMARLARA YÖNELİK SİBER GÜVENLİK

Dijital dünyada güvenlik her geçen gün daha kritik bir hale geliyor. Kurumlar, sürekli artan siber tehditlerle mücadele etmek için yüksek nitelikli güvenlik uzmanlarına ihtiyaç duyuyor. Bu eğitim programı, ağ güvenliği, siber tehdit istihbaratı, penetrasyon testleri ve siber olay müdahale gibi alanlarda uzmanlaşmak isteyen profesyonellere yönelik tasarlanmıştır.

Eğitim, siber güvenlik dünyasının en önemli konularını kapsamlı bir şekilde ele alır. Katılımcılar, günümüzün en gelişmiş siber tehditlerine karşı etkili savunma stratejileri geliştirme ve siber saldırılara karşı kurumlarını koruma becerilerini kazanacaklardır. Ayrıca, uygulamalı laboratuvar çalışmaları ile teorik bilgilerin gerçek dünya senaryolarına nasıl uygulandığını görme fırsatı bulacaklardır.

MİMARLARA YÖNELİK SİBER GÜVENLİK

KURUMSAL ÖZEL EĞİTİM

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

Vebende
Bilişim, Eğitim ve Danışmanlık

MİMARLARA YÖNELİK SİBER GÜVENLİK EĞİTİMİ

Katılımcılar, günümüzün en gelişmiş siber tehditlerine karşı etkili savunma stratejileri geliştirme ve siber saldırılara karşı kurumlarını koruma becerilerini kazanacaklardır. Ayrıca, uygulamalı laboratuvar çalışmaları ile teorik bilgilerin gerçek dünya senaryolarına nasıl uygulandığını görme fırsatı bulacaklardır.

- **Siber Tehdit İstihbaratı ve Tehdit Analizi:** Tehdit aktörlerinin motivasyonlarını anlama, zararlı yazılım analiz teknikleri ve saldırı yüzeyi analizi gibi temel konularda derinlemesine bilgi edinilecek.
- **Ağ Güvenliği ve Güvenlik Duvarı Yapılandırması:** Ağ segmentasyonu, güvenlik duvarı yönetimi, DDoS saldırıları ve IPS/IDS sistemleri gibi ağ güvenliği bileşenlerinin nasıl yapılandırılacağı öğrenilecek.
- **Penetrasyon Testi ve Sızma Testleri:** Gerçek dünya saldırı senaryolarıyla, zafiyetlerin tespiti ve güvenlik açıklarının giderilmesi konusunda pratik beceriler kazanılacak.
- **Uygulama Güvenliği:** Web uygulamaları ve API güvenliği, güvenli kod geliştirme, SQL enjeksiyonu ve XSS gibi yaygın güvenlik açıklarının tespiti yapılacak.
- **Siber Olay Müdahale ve Kriz Yönetimi:** Olay müdahale süreçlerinin etkin yönetimi, kriz anlarında hızlı karar alma ve saldırı sonrası iyileştirme stratejileri gibi kritik konulara odaklanılacak.

EĞİTİM HEDEFİ

Bu eğitim, yazılım ve sistem mimarlarına, siber güvenlik tehditlerini anlamaları, savunma stratejileri geliştirmeleri ve güvenli bir yazılım mimarisi oluşturabilmeleri için gerekli bilgileri kazandırmayı hedefler. Yazılım geliştirme ve sistem tasarımı süreçlerinde güvenlik unsurlarını entegre edebilme, yazılımda güvenlik açıklarını önceden tespit etme ve sistem mimarisinde güvenliği sağlama konularına odaklanacaktır.

EĞİTİM İÇERİĞİ

SİBER TEHDİT İSTİHBARATI VE TEHDİT ANALİZİ

- Siber Tehdit İstihbaratı (CTI): Tehdit istihbaratının tanımı, kaynakları ve kullanımı. Açık kaynak istihbaratı (OSINT) ve tehdit verilerinin nasıl toplandığı ve analiz edildiği.
- Tehdit Aktörleri: Gelişmiş kalıcı tehditler (APT'ler), devlet destekli saldırılar, siber suç grupları ve hacktivistler gibi farklı tehdit aktörlerinin motivasyonları ve teknikleri.
- Zararlı Yazılım Analizi: Zararlı yazılımların (malware) nasıl çalıştığının anlaşılması, tersine mühendislik (reverse engineering) teknikleri ve zararlı yazılımın tespit edilmesi.
- Saldırı Yüzeyi Analizi: Kurumun saldırı yüzeylerinin tespiti, ağ yapısının incelenmesi ve saldırıya açık noktaların belirlenmesi.

AĞ GÜVENLİĞİ VE GÜVENLİK DUVARI YAPILANDIRMASI

- İleri Seviye Ağ Güvenliği: Ağ segmentasyonu, honeypot ve honeynet kullanımı, güvenli veri akışı sağlama teknikleri.
- Güvenlik Duvarı (Firewall) Yönetimi: Güvenlik duvarlarının yapılandırılması, ileri seviye kuralların tanımlanması, trafik izleme ve olay yönetimi.
- Saldırı Tespit ve Önleme Sistemleri (IDS/IPS): IDS ve IPS sistemlerinin çalışma prensipleri, konfigürasyon ve gelişmiş kullanım yöntemleri.
- DDoS Saldırıları ve Koruma Yöntemleri: Dağıtılmış hizmet dışı bırakma (DDoS) saldırılarının türleri ve korunma yöntemleri. Anti-DDoS çözümleri.

PENETRASYON TESTİ VE SIZMA TESTLERİ

- Penetrasyon Testi (Pentest) Nedir? Penetrasyon testinin tanımı, test süreçleri ve aşamaları. Black box, white box ve grey box testlerin farkları.
- Zafiyet Taraması: Kurum içi ve dışı ağlarda zafiyetlerin tespiti, açık kaynak zafiyet tarama araçlarının kullanımı (Nmap, OpenVAS, Nessus).
- Sızma Testi Araçları: Metasploit, Burp Suite, Wireshark gibi ileri seviye sızma testi araçlarının kullanımı ve pratik uygulamaları.
- Gerçek Dünya Senaryoları: Gerçek saldırı senaryolarının canlandırılması, kurum içi sızma testleri ile güvenlik açıklarının tespiti ve iyileştirilmesi.

UYGULAMA GÜVENLİĞİ VE GÜVENLİK AÇIKLARI

- Uygulama Güvenliğine Giriş: Web uygulamaları, mobil uygulamalar ve API güvenliği. Uygulama katmanı güvenlik açıklarının (OWASP Top 10) detaylı incelenmesi.
- Kod Analizi ve Güvenli Kod Geliştirme: Kaynak kod analizi, zafiyetlerin tespiti ve güvenli yazılım geliştirme metodolojileri (DevSecOps).
- Güvenlik Testleri: Web uygulamaları üzerinde güvenlik testleri, SQL enjeksiyonu (SQL Injection), XSS (Cross-Site Scripting) ve CSRF (Cross-Site Request Forgery) gibi yaygın açıkların tespiti.
- İleri Seviye Uygulama Güvenliği: Zero-day zafiyetleri, exploit geliştirme ve güvenlik test otomasyonu.

SİBER OLAY MÜDAHALE VE KRİZ YÖNETİMİ

- Siber Olay Müdahale Süreçleri: Siber olayların tespit edilmesi, raporlanması ve analiz edilmesi. Olay müdahale ekibinin (SOC) görev ve sorumlulukları.
- Olay Müdahale ve Adli Bilişim: Dijital adli bilişim teknikleri, olay sonrasında kanıt toplama, veri kurtarma ve olay analiz süreçleri.
- Kriz Yönetimi ve İş Sürekliliği: Siber saldırılar sırasında kriz yönetimi, iş sürekliliği planlarının hazırlanması ve test edilmesi.
- Saldırı Sonrası İyileştirme: Saldırı sonrası sistemlerin güvenlik seviyesinin artırılması, sistem yamalarının uygulanması ve sürekli izleme stratejileri.

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 iceriğe cevap verir. Katılımcılar bu araçlarla eğitimlerde sorulan sorulara ve taleplere uygun iceriğe 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.

MİMARLARA 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.

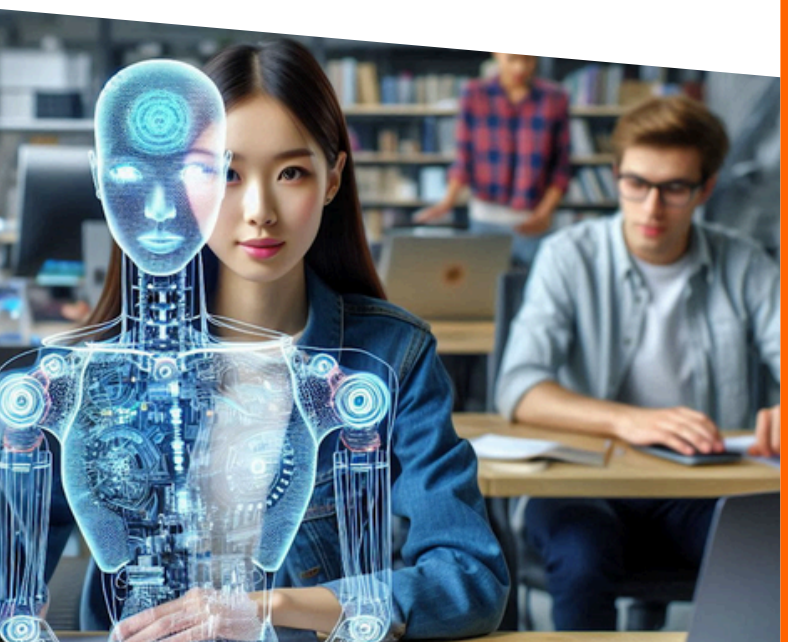
"

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