TÜBİTAK

BİLGEM

BİLİŞİM VE
BİLGİ GÜVENLİĞİ
İLERİ TEKNOLOJİLER
ARAŞTIRMA MERKEZİ

Eğitim Kataloğu

www.bilgem.tubitak.gov.tr

SUNUŞ

TÜBİTAK BİLGEM, bilişim, bilgi güvenliği ve ileri elektronik alanlarında gerçekleştirdiği çalışmalarla ülkemizin ihtiyaçlarına yenilikçi ve milli çözümler üreten ulusal Ar-Ge merkezidir. Merkezimiz, uluslararası standartlarda bilimsel ve teknolojik araştırmalar gerçekleştirmektedir.

Araştırma ve Geliştirme, Test ve Değerlendirme, Prototip Üretimi, Danışmanlık ve Eğitim, BİLGEM'in temel faaliyetleridir. Uzman kadrosu, bilgi birikimi ve yetkinliğiyle BİLGEM, kamu, askeri ve özel kuruluşlara Bilişim ve Bilgi Güvenliği başlıklarında uzmanlık ve kullanıcı eğitimleri vermektedir.

Bu doğrultuda hazırlanan TÜBİTAK BİLGEM Eğitim Kataloğu'nu istifadenize sunarız.

! *Eğitimlerimiz Kurum ve Kuruluşlara sunulmakta olup* ***bireysel başvurular kabul edilmemektedir.***

TÜBİTAK
BİLGEM

NİTELİKLİ ARAŞTIRMA KADROMUZLA,
GÜNCEL TEKNOLOJİYE YÖN VERMEK
VE GELECEĞİN TEKNOLOJİSİNİ
ŞEKİLLENDİREBİLMEK ADINA ÇIKTIĞIMIZ YOLDA
EMİN ADIMLARLA İLERLİYORUZ.

İçindekiler

TDBY EĞİTİMLERİ

Test ve Değerlendirme Başkan Yardımcılığı

TDBY
TEMPEST EĞİTİMLERİ

1. GENEL TEMPEST EĞİTİMİ

Eğitimin Süresi	1 gün
Ön Şartlar	Bilgi güvenliği konusunda bilgi sahibi olmak.
Kimler Katılabilir?	• Bilgi güvenliği konusunda çalışanlar, • Muhabereciler, • TEMPEST (bilgi kaçakları) konusunda bilgi sahibi olmak isteyenler, • BT ürünlerini ve sistemlerini denetleme, tasarlama/geliştirme, kullanma rollerine sahip kişiler.
Eğitim Hedefleri	• Bilgi güvenliği ve TEMPEST kavramlarının neler olduğunun öğrenilmesi, • TEMPEST'in tarihçesinin öğrenilmesi, • TEMPEST ile ilgili standartlar hakkında bilgi sahibi olunması, • Bilgi kaçağını engelleme amaçlı ne gibi tedbirlerin alınması gerektiği hakkında kazanımlar.
Konu Başlıkları	• Bilgi Güvenliği • TEMPEST Nedir? • TEMPEST Tarihçesi • Tanımlar ve Önemli Kavramlar • Cihaz TEMPEST Riskleri • TEMPEST Standartları • TEMPEST Politikası • TEMPEST Karşı Tedbirler

2. TEMPEST GENEL TESİSAT REHBERİ EĞİTİMİ

Eğitimin Süresi	0.5 gün
Ön Şartlar	Bilgi güvenliği konusunda bilgi sahibi olmak.
Kimler Katılabilir?	• Bilgi güvenliği konusunda çalışanlar, • Muhabereciler, • TEMPEST (bilgi kaçakları) konusunda bilgi sahibi olmak isteyenler, • BT ürünlerini ve sistemlerini denetleme, tasarlama/geliştirme, kullanma rollerine sahip kişiler.
Eğitim Hedefleri	• Bilgi güvenliği ve TEMPEST bina ve cihaz değerlendirmesinin, • Kırmızı ve siyah kavramlarının, • Sabit ve hareketli tesislerde TEMPEST uyumlu tesisatın nasıl yapılacağının, • Genel tesisat kurallarını ve tesisat şartlarının neler olduğunun, • TEMPEST önlemlerinin neler olduğunun öğrenilmesi.
Konu Başlıkları	• Bina Değerlendirmesi • Cihaz Değerlendirmesi • Uygun Tesisat Nasıl Yapılır? • Kırmızı ve Siyah Kavramları • Genel Tesisat Kuralları • Tesisat Şartları • TEMPEST Önlemleri

TDBY
YTKDL EĞİTİMLERİ

1. YAZILIM TEST EĞİTİMİ

Eğitimin Süresi	1 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• Yazılım test mühendisleri, • Yazılım geliştiriciler, • Proje yöneticileri, • İş analistleri, • Sistem mühendisleri.
Eğitim Hedefleri	• Yazılım testi kavramlarının, • Yazılım felaketleri ile yazılım testlerinin öneminin, • Yazılım geliştirme projelerinde yazılım testlerinin nasıl yapılacağının, test sürecinin nasıl işletileceği ve yönetileceğinin, yazılım test tekniklerinin, gözden geçirmelerinin, test dokümantasyonu ve test otomasyonu konularının öğrenilmesi.
Konu Başlıkları	• Yazılım Testinin Temelleri ve Önemi • Yazılım Felaketleri • Yazılım Yaşam Döngüsünde Test • Yazılım Gereksinim Analizi • Yazılım Test Seviyeleri • Yazılım Test Teknikleri • Test Dokümantasyonu • Test Otomasyonu • Test Yönetimi ve Hata Yaşam Döngüsü • Test Standartları • Gözden Geçirme Süreci • Pratik Uygulamalar/Öğrenilen Dersler

2. YAZILIM KALİTE METRİKLERİ

Eğitimin Süresi	0.5 gün
Ön Şartlar	Temel programlama bilgisine sahip olmak.
Kimler Katılabilir?	• Yazılım test mühendisleri, • Yazılım geliştiriciler, • Proje yöneticileri, • İş analistleri, • Sistem mühendisleri.
Eğitim Hedefleri	• Kaliteli kod yazmanın getireceği zorluk ve maliyet yanında kazandıracaklarının öneminin kavranması, • Kod kalitesini arttırmanın önemi, • Koda ve projeye hakim olmanın yolunun iyi bir ölçüm ve değerlendirme mekanizması sayesinde gerçekleşebileceğinin kavranması.
Konu Başlıkları	• Yazılım Kod Kalitesini Etkileyen Faktörler • Yazılımda Hataların Ortaya Çıkarılması ve Giderilmesi - Statik Yöntemler (Gözden Geçirmeler, Kod Analizi vs.) - Dinamik Yöntemler (Birim Testler, Sistem Testleri vs.) • Ölçme Süreçleri ve Yöntemleri • Statik Kod Analizi • Yazılım Metrikleri - Karmaşıklık Metrikleri - Satır Sayısı Metrikleri - Nesne Yönelimli Metrikler - Halstead Metrikleri - Bakım Yapılabilirlik Metrikleri - Paket Metrikleri • Araçlar ve Teknikler • Karmaşıklık İndirgeme • Ölçme Sürecinin Otomasyonu

3. STATİK KOD ANALİZİ İLE KRİTİK UYGULAMA AÇIKLARININ TESPİTİ

Eğitimin Süresi	0.5 gün
Ön Şartlar	Temel programlama bilgisine sahip olmak.
Kimler Katılabilir?	• Yazılım geliştiriciler, • Yazılım test mühendisleri, • Proje yöneticileri, • Yazılım kalite mühendisleri.
Eğitim Hedefleri	• Güvenli kod geliştirmek için hangi kılavuzlardan faydalanacaklarının, • Kod geliştirirken hatalardan kaçınma yöntemlerinin, kod iyileştirmeye yönelik temel bilgilerinin edinimi.
Konu Başlıkları	• Statik Kod Analizi Nedir? • Uluslararası Kod Güvenlik Rehberleri Nelerdir? - OWASP, SANS, CWE • En Çok Karşılaşılan Kodlama Sorunları - En Çok Yapılan Hatalar - Örnekler Üzerinden Anlatım • Kodlama Dillerine Özgü Öne Çıkan Sorunlar • Araçlar • Pratik Kod İyileştirme Örnekleri

4. YAZILIM GÜVENİLİRLİĞİ VE GÜVENİLİR YAZILIM GELİŞTİRME SÜREÇLERİ

Eğitimin Süresi	1 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• Yazılım geliştiriciler, • Yazılım test mühendisleri, • Proje yöneticileri, • Yazılım kalite mühendisleri.
Eğitim Hedefleri	• Güvenilirlik kavramının, • Yazılım kalitesi, yazılım testleri ve güvenilirliliğin, • Yazılımın güvenilirliğini arttırmanın öneminin, • Güvenilirlik modellerinin, • Güvenilirlik için gerekli ölçümlerin öğrenimi.
Konu Başlıkları	• Yazılım Güvenilirliği ve Güvenilir Yazılım Geliştirme • Emniyet, Güvenilirlik ve Güvenlik Tanımları • Hata Yoğunluğu Öngörüsü (Prediction) ve Arıza (Sorun) Tahmini (Estimation) • Yazılım Güvenilirlik Modelleri • Bir Teknik Performans Metriği Olarak Güvenilirlik - Roma Lab. Modeli • Emniyet Kritik Yazılım Geliştirme Süreçleri - DO 178 C Tanıtımı, Seviyeleri ve Amaçları - CENELEC 50128 Tanıtımı, Seviyeleri ve Amaçları

5. KULLANILABİLİRLİK EĞİTİMİ

Eğitimin Süresi	0.5 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• Yazılım test mühendisleri, • Yazılım geliştiriciler, • Proje yöneticileri, • İş analistleri, • Kullanıcı grafik arayüz tasarımcıları.
Eğitim Hedefleri	• Kullanılabilirlik ve kullanıcı deneyimi kavramlarının öğrenimi, • Kullanılabilirlik değerlendirme ve test yöntemlerinin kavranması, • Kullanılabilir yazılım geliştirmenin öneminin kavranması, • Standartlara ve rehberlere uygun yazılımların geliştirilmesi.
Konu Başlıkları	• Kullanılabilirlik ve Kullanıcı Deneyimi • Kullanılabilirlik Problemleri • Kullanıcı Merkezli Tasarım • Kullanılabilirlik Testi ve Yöntemleri • Göz İzleme Uygulaması • Kullanılabilirlik Değerlendirmesi ve Yöntemleri • Kullanılabilirlik Standartları ve Rehberleri • Pratik Uygulamalar/Öğrenilen Dersler • 50128 Tanıtımı, Seviyeleri ve Amaçları

6. PERFORMANS TEST EĞİTİMİ

Eğitimin Süresi	0.5 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• Yazılım test mühendisleri, • Yazılım geliştiriciler, • Proje yöneticileri, • İş analistleri, • Sistem mühendisleri.
Eğitim Hedefleri	• Yazılımın performansının nasıl belirleneceğinin tanımlanması, • Yazılımların performansını etkileyen faktörlerin tanımlanması, • Yazılım performans testlerinde dikkat edilmesi gereken hususların öğrenilmesi.
Konu Başlıkları	• Performans Testinin Temelleri • Performans Gereksinimleri • Performans Test Çeşitleri • Performansı Etkileyen Faktörler Kullanılan Araçlar • Performans Test Süreci • Performans Testlerinde Yaşanan Riskler • Sorunlar ve Çözüm Önerileri

7. RAFTA HAZIR TİCARİ ÜRÜNLER (TSE ISO EN 25051) SERTİFİKASYONU

Eğitimin Süresi	0.5 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• Yazılım geliştiricileri, • Yazılım tedarikçileri, • Yazılım test ve kalite mühendisleri, • Proje yöneticileri, • Cots ürünü satın alacak müşteriler.
Eğitim Hedefleri	• TS ISO/IEC 25051 standardı ve yazılım kalitesinin öneminin kavranması, • TS ISO/IEC 25051 Standardı içeriği, standarda uygunluk değerlendirme süreci ve yöntemleri konusunda farkındalık oluşturulması, • COTS (RUSP) ürün satın alacak kişiler/kurumlar için güvenin oluşması ve memnuniyetin artırılması.
Konu Başlıkları	• TS ISO/IEC 25051 Standardı Önemi - Yazılım Kalitesinin Önemi - Yazılım Testinin Önemi • TS ISO IEC 25051 Standardına Genel Bakış • TS ISO IEC 25051 Standardı İçeriği • COTS Yazılım Ürünü Gereksinimleri - Ürün Açıklaması Gereksinimleri - Kullanıcı Dokümantasyonu Gereksinimleri - Yazılım için Kalite Gereksinimleri Kullanılan Araçlar • Test Dokümantasyonu için Gereksinimler - Test Planı Gereksinimleri - Test Açıklamaları Gereksinimleri - Test Sonuçları Gereksinimleri • Standarda Uygunluk Değerlendirme Yöntemleri • Standarda Uygunluk Değerlendirme Süreci

8. ELEKTRONİK BELGE YÖNETİMİ (TSE ISO EN 13298) SERTİFİKASYONU

Eğitimin Süresi	0.5 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• EBYS yazılım geliştiricileri, • EBYS yazılım tedarikçileri, • EBYS yazılım test mühendisleri, • Proje yöneticileri, • EBYS ürünü satın alacak müşteriler.
Eğitim Hedefleri	• EBYS belge yönetim tekniklerini ve uygulamalarının öğrenimi, • EBYS gereksinimlerinin kavranması, • Sertifikasyon sürecinde gerçekleştirilecek faaliyetlerin öğrenimi.
Konu Başlıkları	• EBYS için Gerekli Belge Yönetim Teknikleri ve Uygulamaları • Elektronik Belgelerin Yönetilebilmesi için Gerekli Gereksinimler • Elektronik Ortamda Üretilmemiş Belgelerin Yönetim Fonksiyonlarının Elektronik Ortamda Yürütülebilmesi için Gerekli Gereksinimler • Elektronik Belgelerde Bulunması Gereken Diplomatik Özellikler • Elektronik Belgelerin Hukuki Geçerliliklerinin Sağlanması için Alınması Gereken Önlemler • Güvenli Elektronik İmza ve Mühür Sistemlerinin Uygulanması için Gerekli Sistem Altyapısı • Sertifikasyon Sürecinde Yapılması Gerekenler

1. ORTAK KRİTERLER (TS ISO/IEC 15408) EĞİTİMİ

Eğitimin Süresi	1 gün
Ön Şartlar	Ortak Kriterler standardı Bölüm-1'in "Introduction and General Model" (Giriş ve Genel Model) eğitimden önce gözden geçirilmesi, eğitimin daha verimli olmasını sağlayacaktır.
Kimler Katılabilir?	• Bilişim teknolojisi (BT) ürünlerini ve sistemlerini denetleyenler, • BT ürünlerini tasarlama/geliştirme ve kullanma sorumluluğuna sahip kişiler.
Eğitim Hedefleri	• Ortak Kriterler standardı, kullanımı, uygulamaları setifikasyon süreci hakkında temel bilgilere sahip olunması.
Konu Başlıkları	• Ortak Kriterler Standardı, Uygulama Alanı ve Standardın Bölümleri Hakkında Özet Bilgi • Ortak Kriterler Standardının, BT Ürün/Sistem Denetçileri, Tasarımcıları ve Tüketicileri Tarafından Nasıl Kullanılabileceği • Türkiye'deki Ortak Kriterler Yapısı (Sertifika Makamı - Laboratuvar), Ortak Kriterler Değerlendirme Süreci ve Ortak Kriterler Sertifika Yayınlama Süreci • Uluslararası Alanda Ortak Kriterler Standardının Yaygınlığı • Ortak Kriterler Standardına Uygun Olarak Güvenlik, Kullanılabilirlik, Bütünlük ve Güvenilirlik Değerlendirmesi Gerçekleştirilebilecek Olan BT Ürün ve Sistem Türleri (Akıllı Kart, Sınır Koruma Cihazları, İşletim Sistemleri vb.)

2. AKILLI KART YAN KANAL ANALİZİ VE TERSİNE MÜHENDİSLİK EĞİTİMİ

Eğitimin Süresi	5 gün (1 gün teorik, 4 gün pratik)
Ön Şartlar	RSA (Rivest Shamir Adleman), DES (Data Encryption Standard) ve AES (Advanced Encryption Standard) kripto algoritmalarının işleyişi ile ilgili temel düzeyde bilgiye sahip olunması.
Kimler Katılabilir?	• Bilişim teknolojisi (BT) ürünlerini ve sistemlerini denetleyenler • BT ürünlerini tasarlama/geliştirme ve kullanma sorumluluğuna sahip kişiler
Eğitim Hedefleri	• Akıllı kartlar için gerçeklenebilir olan Yan Kanal Analizi hakkında bilgi sahibi olunması, • Akıllı kartlar için Tersine Mühendislik saldırı teknikleri hakkında bilgi sahibi olunması, • Saldırı tekniklerine karşı alınabilecek önlemler hakkında bilgi sahibi olunması.
Konu Başlıkları	Teorik Bölüm: • Yan Kanal Analizi (Side Channel Analysis) Saldırı Teknikleri • Tersine Mühendislik (Reverse Engineering) Saldırı Teknikleri Pratik Bölüm: • RSA Algoritması Basit Güç Analizi (Simple Power Analysis) • RSA Algoritması Farksal Güç Analizi (Differential Power Analysis) • AES Algoritması Güç Analizi (Power Analysis) • DES Algoritması Güç Analizi • RSA Algoritması Hata Analizi (Fault Analysis) • DES Algoritması Hata Analizi • AES Algoritması Hata Analizi • Odaklanmış İyon Işını (Focused Ion Beam) Cihazı ile Akıllı Kart Veri Yolu Dinleme (Bus Probing) ve Yonga Biçimlendirme (Circuit Edit)

1. HEDEF SINIFLANDIRMA EĞİTİMİ

Eğitimin Süresi	1 gün
Ön Şartlar	Temel matematik, lineer cebir, olasılık teorisi ve temel seviyede optimizasyon bilgisine sahip olmak.
Kimler Katılabilir?	• Radar hedef sınıflandırma alanında araştırma yapan bilim insanları veya mühendisler
Eğitim Hedefleri	• Hedef sınıflandırma hakkında genel bilgi ve beceri kazanımı, • Hedef sınıflandırma ile ilgili temel teorik bilgilerin edinimi, • Hedef sınıflandırma problemlerinin tanımlanması ve tasarlanmasına yönelik kabiliyetlerin kazanımı
Konu Başlıkları	• Hedef Sınıflandırma Temelleri • Öznitelik Kavramı • Öznitelik Üretimi, Öznitelik Seçimi Ve Boyut Azaltımı • Parametre Kestirimi • Bayes Karar Kuralı Tabanlı Sınıflandırıcılar • Lineer Sınıflandırıcılar • Lineer Olmayan Sınıflandırıcılar • Saklı Markov Modelleri • Öğreticisiz Sınıflandırma

GİRİŞ SEVİYESİ EĞİTİMLERİ

STANDART SEVİYE EĞİTİMLER

SGE Siber Güvenlik Enstitüsü EĞİTİMLERİ

GELİŞMİŞ SEVİYE EĞİTİMLER

İLERİ SEVİYE EĞİTİMLER

SGE

GİRİŞ SEVİYESİ EĞİTİMLER

1. KULLANICI GÜVENLİĞİ

Eğitimin Süresi	3 saat
Ön Şartlar	Bilgi sistemlerini normal bir kullanıcı olarak kullanma bilgisine sahip olmak.
Kimler Katılabilir?	• Bilgi sistemlerini kullanan kullanıcılar.
Eğitim Hedefleri	• Bilgi güvenliğinin önemi konusunda bilinçlenme, • Bilgi güvenliği yönetim sisteminin bir parçası olarak sorumluluk ve görevler hakkında bilgi edinimi, • Bilgi güvenliğine ilişkin temel bilgilerin edinimi.
Konu Başlıkları	• Bilgi Güvenliğinde Kullanıcının Rolü • Kurum Bilgi Güvenliği Yönetim Sisteminde Kullanıcının Yeri • Bilgisayarlara Erişim • Parola Güvenliği • E-Posta Güvenliği • İnternet Erişim Güvenliği • Virüs Koruma • Bilgi Ortamlarının Oluşturulması, Değiştirilmesi ve Yok Edilmesi • Dosya Erişim ve Paylaşımı • Veri Yedeklemesi • Sosyal Mühendislik • Acil Durumlarda Kullanıcının Uyması Gereken Prensipler

2. YÖNETİCİLERE ODAKLI GENEL GÜVENLİK

Eğitimin Süresi	2 gün
Ön Şartlar	Bilgi sistemleri hakkında genel bilgi sahibi olmak.
Kimler Katılabilir?	• Bilgi güvenliği ile ilgili bilgi almak isteyen yöneticiler, • Bilgi sistemleri ile ilgili genel bilgisi olup bilgi güvenliği konusunda bilgi edinmek isteyen kişiler.
Eğitim Hedefleri	• Bilgi güvenliğinin genel kavramları ve bilgi güvenliği yönetim sisteminin genel yapısı hakkında bilgi edinimi, • Sistem güvenliği hakkında temel teknik bilgilerin edinimi.
Konu Başlıkları	• Bilgi Güvenliği Temel Kavramları • Güvenlik Politikası • Bilgi Güvenliği Organizasyonu • Personel Güvenliği • Risk Analizi ve Risk Yönetimi • İş Sürekliliği • Güvenlik Olayları Müdahalesi • İşletim Sistemi Güvenliği • Ağ Güvenliği • Web Güvenliği • Dijital Sertifikalar ve Sertifika Dağıtım Sistemleri • Parola Yönetimi • Virüs Koruma Sistemleri

3. SOSYAL MÜHENDİSLİK: SALDIRI VE KORUNMA YÖNTEMLERİ

Eğitimin Süresi	2 gün
Ön Şartlar	Eğitim uygulamalı olarak yapılacağından, eğitim sınıfında katılımcı sayısı kadar bilgisayar bulunması gerekmektedir.
Kimler Katılabilir?	• Sistem yöneticileri öncelikli olmak üzere tüm bilgisayar kullanıcıları.
Eğitim Hedefleri	• Sosyal mühendislik saldırılarına karşı bağışıklık kazanımı, • Kendi kurumunda benzer bir eğitimi verecek bilgi birikiminin edinimi.
Konu Başlıkları	• Sosyal Mühendislik Kavramı • Saldırı Teknikleri • Sosyal Mühendislik Saldırı Örnekleri • Sosyal Mühendislik Testleri • Korunma Yöntemleri • Çeşitli Sosyal Mühendislik Uygulamaları

1. BİLGİ GÜVENLİĞİNE GİRİŞ

Eğitimin Süresi	10 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• Bilgi güvenliğinin tüm alanları ile ilgili temel bilgi almak isteyen kişiler.
Eğitim Hedefleri	• Bilgi güvenliği temel konularında bilgi edinimi, • Windows güvenliği, linux güvenliği ve siber tehditler gibi farklı alanlarda bilgi sahibi olarak bilgi güvenliğine bütüncül bir bakış açısı kazanımı.
Konu Başlıkları	• Bilgi Güvenliğine Giriş, Temel Kavramlar • TCP/IP • Güvenlik Cihazları ve Yöntemler • Kriptografiye Giriş • Unix/Linux Güvenliği • Windows Güvenliği • Web Güvenliği • Kablosuz Ağ Güvenliği • Sosyal Mühendislik • Kayıt Yönetimi • Olay Müdahale • Zararlı Yazılımlar, Bulaşma Teknikleri ve Analizi • Siber Saldırı Çeşitleri • Gelişmiş Siber Tehditler

SGE
STANDART SEVİYE EĞİTİMLER

2. ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMA

Eğitimin Süresi	3 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır. Kalite sistemleri ile tanışıklık avantaj sağlamaktadır.
Kimler Katılabilir?	• ISO 27001 tabanlı Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak ve işletmekle sorumlu kişiler, • ISO 27001 denetimine tâbi olacak veya denetime katılacak kişiler.
Eğitim Hedefleri	• BGYS kurma kabiliyetinin kazanımı, • Denetime ilişkin kavramlar ile ilgili bilgi edinimi.
Konu Başlıkları	• Bilgi Güvenliği Yönetim Sistemi Nedir? Neden Gereklidir? • ISO 27001'de "Planla-Uygula-Kontrol Et-Önlem Al" Döngüsü • Bilgi Sistemi Risk Analizi ve Tedavisi • ISO 27001 Temel Kontrol Alanları - Güvenlik Politikaları - Bilgi Güvenliği Organizasyonu - İnsan Kaynakları Güvenliği - Varlık Yönetimi - Erişim Kontrolü - Kriptografi - Fiziksel ve Çevresel Güvenlik - İşletim Güvenliği - Haberleşme Güvenliği - Sistem Temini, Geliştirme ve Bakımı - Tedarikçi İlişkileri - Bilgi Güvenliği İhlâl Olayı Yönetimi - İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları - Uyum • ISO 27001'e Uygunluk Denetimi - Denetim Planlama - Denetim Kontrol Listeleri - Uygunsuzluklar ve Raporlama • Çeşitli Uygulamalar

3. YÖNETİCİLERE ODAKLI ISO 27001 BİLGİLENDİRME

Eğitimin Süresi	3 saat
Ön Şartlar	Belirli bir ön şart bulunmamaktadır. Kalite sistemleri ile tanışıklık avantaj sağlamaktadır.
Kimler Katılabilir?	• ISO 27001 tabanlı Bilgi Güvenliği Yönetim Sistemi (BGYS) ile ilgili bilgi edinmek isteyen yöneticiler.
Eğitim Hedefleri	• Eğitime katılanlar ISO 27001 ve BGYS hakkında genel bilgi sahibi olacaktır.
Konu Başlıkları	• Bilgi Güvenliği Yönetim Sistemi Nedir? Neden Gereklidir? • Standart Tarihçesi • Annex SL Yapısı • PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) Yakıştırımı • Standartta Yer Alan Zorunlu Maddeler • Ek A: Referans Kontrol Amaçları ve Kontroller • Standarda Uyumluluk Sürecinde Dikkat Edilmesi Gereken Hususlar

4. SİBER OLAYLARA MÜDAHALE EKİBİ

Eğitimin Süresi	2 gün
Ön Şartlar	Hem idari süreçler, hem bilgi sistemleri altyapısı konularında orta derecede tecrübe sahibi olmak.
Kimler Katılabilir?	• Kurumlarında SOME (Siber Olaylara Müdahale Ekibi) biriminin kurulması/yönetilmesi konusunda görev alacak personel, • Kurumda bilgi güvenliği birimlerinde çalışan personel.
Eğitim Hedefleri	• Kurumlarında siber olaylara müdahale sürecini oluşturacak kabiliyetlerin edinimi.
Konu Başlıkları	• Giriş (Tarihçe, Örnek Bilgisayar Olayları, Ulusal Siber Olaylara Müdahale Organizasyonu) • SOME Temel Konuları (SOME Nedir, Kurum İçi Paydaşları Kimlerdir?) • SOME Kurulum Aşamaları • SOME'lerin Görev ve Sorumlulukları - Siber Olay Öncesinde - Siber Olay Esnasında Müdahale Süreci - Siber Olay Sonrası • SOME Operasyonel Elemanları (Yazılım, Donanım, Politika ve Prosedürler)

5. KRİTİK ALTYAPILARIN KORUNMASI

Eğitimin Süresi	2 gün
Ön Şartlar	Kendi kurumunun iş süreçlerine yakınlık, bilişim sistemleri ve bilgi güvenliği konusunda temel bilgi sahibi olmak.
Kimler Katılabilir?	• Kritik altyapı işleten kurumların yöneticileri, • Kurumsal SOME ve Bilgi İşlem birimi sorumluları ve çalışanları.
Eğitim Hedefleri	• Kritik altyapıların ve Endüstriyel Kontrol Sistemlerinin kendine has önemi ve alınması gereken önlemler hakkında bilgi edinimi, • Kurumların kritik altyapıların güvenliğine ilişkin hem idari süreci, hem teknik önlemleri uygulama konusunda yetkinlik kazanmaları.
Konu Başlıkları	• Kritik Altyapılar ve Bilgi Sistemleri • Kritik Altyapılar ve Bilgi Güvenliği Olayları • Kurumlarda Bilgi Güvenliğinin Yönetilmesi (Tehditler ve Önlemler) • Ulusal Boyutta İşletmeciler ve Düzenleyiciler • Ulusal Siber Güvenlik Organizasyonu • Dünyadaki Durum ve Türkiye için Öneriler

6. WINDOWS GÜVENLİĞİ

Eğitimin Süresi	3 gün
Ön Şartlar	Temel Windows ve ağ bilgisi hakkında bilgi sahibi olmak.
Kimler Katılabilir?	• Windows ağ yöneticileri, • Microsoft Aktif Dizin yöneticileri, • Microsoft sistemlerine güvenli bir geçiş yapmayı planlayanlar, • Microsoft sistemlerinde güvenlik konusuna ilgi duyanlar.
Eğitim Hedefleri	• Windows güvenliği konusunda temel bilgi edinimi, • Kurumlarında windows güvenliği alanında uygulama yapabilecek kabiliyetlerin kazanımı.
Konu Başlıkları	• Windows İşletim Sistemi Güvenliği • IPSec, PKI (“Public Key Infrastructure” – Açık Anahtar Altyapısı) ve EFS (“Encrypting File System” – Şifreli Dosya Sistemi) • Windows Ortamında “Powershell” Geliştirme

7. MICROSOFT SİSTEMLERİ GÜVENLİĞİ

Eğitimin Süresi	4 gün
Ön Şartlar	Temel Windows, Exchange, aktif dizin ve ağ bilgisi hakkında bilgi sahibi olmak.
Kimler Katılabilir?	• Windows ağ yöneticileri, • Microsoft Aktif Dizin yöneticileri, • Microsoft sistemlerine güvenli bir geçiş yapmayı planlayanlar, • IIS ve Exchange yöneticileri, • Microsoft sistemlerinde güvenlik konusuna ilgi duyanlar.
Eğitim Hedefleri	• Microsoft sistemleri güvenliği konusunda ileri düzeyde bilgi edinimi, • Kurumlarında microsoft sistemleri güvenliği alanında uygulama yapabilecek kabiliyetlerin kazanımı.
Konu Başlıkları	• Microsoft Web Servisleri Güvenliği • Microsoft “PowerShell” • Aktif Dizin ve Ağ Servisleri Güvenliği (Grup politikası, DNS, DHCP) • Microsoft Sistemlerinde Yama Yönetimi

SGE
STANDART SEVİYE EĞİTİMLER

8. LINUX GÜVENLİĞİ

Eğitimin Süresi	3 gün
Ön Şartlar	Linux sistemlerde sistem yöneticiliği seviyesinde deneyime sahip olmak.
Kimler Katılabilir?	• Linux tabanlı sistemleri güvenli hale getirmek isteyen güvenlik uzmanları, • Linux tabanlı internet uygulamalarının güvenliğinden sorumlu sistem yöneticileri, • Güvenlik testi ve sıkılaştırma araçları konusunda meraklı sistem yöneticileri.
Eğitim Hedefleri	• Linux tabanlı işletim sistemlerinin güvenlik sıkılaştırmasını yapma kabiliyetinin kazanımı, • Linux tabanlı açık kaynak kodlu güvenlik araçlarını kullanma yeteneğinin kazanımı, • Linux sistemlerde güvenlik ihlallerini tespit eden araçları kullanma kabiliyetinin kazanımı.
Konu Başlıkları	• Güvenli Kurulum • Açılış Servisleri Yapılandırması • Çekirdeğin Güvenli Olarak Yapılandırması • Dosya Sistemi Erişim Kontrolü • Kullanıcı Erişim Denetimi • Sistem Kayıtlarının Tutulması • Güvenlik Denetleme Araçları • Güvenlik Sıkılaştırma Araçları • Güvenlik Amaçlı Betik Programlama

9. TCP/IP AĞ GÜVENLİĞİ

Eğitimin Süresi	2 gün
Ön Şartlar	Temel ağ bilgisine sahip olmak.
Kimler Katılabilir?	• Sistem ve ağ yöneticileri, • Güvenlik ve sızma testi uzmanları, • Bilişim sistemleri güvenliği bölümü çalışanları, • Bilgi sistemleri denetleme birimi çalışanları.
Eğitim Hedefleri	• TCP/IP ağ güvenliği konusunda laboratuvar çalışmaları ile bilgi ve yetkinlik kazanımı.
Konu Başlıkları	• TCP/IP Protokol Yığıtında Yer Alan Protokoller • TCP/IP Yığıtının Farklı Katmanlarının Çalışma Şekilleri ve Bunları Hedef Alan Güvenlik Tehditleri • TCP/IP Protokolleri ile İlgili Güvenlik Zafiyetleri ve Çözüm Yolları • Ağ Güvenliğini Sağlamak için Kullanılan Teknikler, Protokoller ve Aygıtlar • Wireshark vb. Paket Yakalama Programları, Protokol ve Paket Yapılarının İncelenmesi • SSL, IPSec, VPN, Sayısal Sertifika Gibi Kavramlar • Firewall, IDS/IPS, Proxy Gibi Ağ Bileşenleri

10. AKTİF CİHAZ GÜVENLİĞİ

Eğitimin Süresi	2 gün
Ön Şartlar	Temel ağ bilgisine sahip olmak.
Kimler Katılabilir?	• Sistem ve ağ yöneticileri, • Güvenlik ve sızma testi uzmanları, • Bilişim sistemleri güvenliği bölümü çalışanları, • Bilgi sistemleri denetleme birimi çalışanları.
Eğitim Hedefleri	• Aktif cihaz güvenliği kapsamında laboratuvar çalışmaları ile bilgi ve yetkinlik kazanımı.
Konu Başlıkları	• Aktif cihaz kavramı ve ağ tasarımı ile aktif cihazların sıkılaştırılması ve ağ altyapısının güvenliğinin sağlanması, kapsamında aşağıdaki başlıklar açıklamalı ve uygulamalı olarak anlatılacaktır: • Günümüzde yaygın olarak kullanılan, iç ağ altyapısını oluşturan ve ağın dış dünya ile bağlantısını sağlayan - Ağ Anahtarı, - Yönlendirme Cihazları, - Güvenlik Duvarı, - İçerik Kontrolcüsü gibi aktif cihazların sıkılaştırmalarına yönelik adımlar • Aktif cihazların üstünde alınabilecek - Fiziksel Güvenlik, - Çalışma Koşulları, - Kimlik Doğrulama, - Yetkilendirme, İzleme, Servis Kontrolü, - Yama Kontrolü, - Erişim Listesi Kontrolü, - Uzaktan Yönetim Kontrolü, vb. güvenlik önlemleri

11. SİSTEM GÜVENLİK DENETİMİ

Eğitimin Süresi	4 gün
Ön Şartlar	Temel ağ bilgileri, işletim sistemleri bilgisi (Windows ve Unix), sınır güvenliği yapılarını tanıma konularında bilgi sahibi olmak.
Kimler Katılabilir?	• Bilgi teknolojileri denetçileri, • Sistem güvenlik denetleme bilgilerini artırmak isteyen bilgi güvenliği uzmanları, • Güvenlik denetim mantığını anlamak ve bu tür denetimlere sistemlerini hazırlamak isteyen sistem ve ağ yöneticileri.
Eğitim Hedefleri	• Güvenlik açıklık tarayıcılarını kullanım yeteneğinin kazanılması, • Linux ve Windows İşletim sistemlerinin, sınır güvenliği bileşenlerinin güvenlik denetimini yapma kabiliyetinin kazanılması.
Konu Başlıkları	• Açıklık, Tehdit Tanımları • Açık Kaynak Kodlu Güvenlik Açıklık Tarayıcıları ve Bu Araçların Kullanımı • Bir Ağın Topolojisini Çıkartma • Sınır Sistemleri Denetimi • Windows Denetimi • Unix/Linux Sistemlerin Denetimi

12. TEMEL GÜVENLİK DENETİMİ

Eğitimin Süresi	1 gün
Ön Şartlar	Temel ağ bilgileri, temel işletim sistemi bilgisine (Windows) sahip olmak.
Kimler Katılabilir?	• Bilgi teknolojileri denetçileri, • Sistem güvenlik denetleme bilgilerini artırmak isteyen bilgi güvenliği uzmanları, • Güvenlik denetim mantığını anlamak ve bu tür denetimlere sistemlerini hazırlamak isteyen sistem ve ağ yöneticileri.
Eğitim Hedefleri	• Güvenlik açıklık tarayıcılarını kullanma yeteneği kazanma, • Windows işletim sistemlerini denetleme kabiliyeti kazanma.
Konu Başlıkları	• Açıklık, Tehdit Tanımları • Açık Kaynak Kodlu Güvenlik Açıklık Tarayıcıları ve Bu Araçların Kullanımı - Nessus, Nmap, MBSA • Windows Denetimi - Güvenlik Şablonları - “Security Configuration and Analysis”-“Güvenlik Analizi ve Yapılandırma” Aracı

13. KABLOSUZ AĞ GÜVENLİĞİ

Eğitimin Süresi	2 gün
Ön Şartlar	Temel ağ bilgisine sahip olmak.
Kimler Katılabilir?	• Kablosuz ağ sistemlerini yöneten veya bu tür sistemleri kurmak isteyen sistem ve ağ yöneticileri, • Kablosuz ağ güvenliği hakkında bilgi almak isteyen bilgi teknolojisi uzmanları.
Eğitim Hedefleri	• Kablosuz erişim riskleri ve bu risklerin nasıl ortadan kaldırılacağı ile ilgili bilgi edinimi, • Kablosuz ağ denetim araçlarını kullanma kabiliyetinin edinimi.
Konu Başlıkları	• Kablosuz Erişim Sağlayan Yerel Alan Ağlarındaki Güvenlik Riskleri • Güvenli Kablosuz İletişim Mimarisi • Kablosuz Ağlarda, Güvenlik ya da Saldırı Amaçlı Kullanılan Yazılımlar

14. KAYIT YÖNETİMİ

Eğitimin Süresi	2 gün
Ön Şartlar	Temel işletim ve bilgi sistemleri bilgisine sahibi olmak.
Kimler Katılabilir?	• Sistem, güvenlik ve ağ yöneticileri, • Bilgi ve bilişim sistemleri uzmanları, • Bilgi güvenliği yöneticileri ve uzmanları.
Eğitim Hedefleri	• Günümüzde gerek yasal sorumluluk, gerekse kurum politikası gereği bilgi teknolojilerinden kayıt (log) bilgisi toplanması ve toplanan bu kayıtların kurum ihtiyaçları doğrultusunda anlamlı hale getirilmesi için etkin ve verimli şekilde yönetilmesini sağlayacak bir kayıt yönetim sisteminin kurulması bilgi ve becerisinin kazanımı.
Konu Başlıkları	• Kayıt Yönetimi ile İlgili Temel Kavramlar • Kayıtları Toplayabilmek için Yerine Getirilmesi Gereken Yapılandırma Ayarları • Toplanan Kayıtlarla İlgili Analiz Teknikleri • Kayıt Yönetim Sistemi Kurulmasında Dikkat Edilecek Hususlar • Büyük Boyutlu Kayıtların Analizi • Toplanan Kayıtların Anlık Takibi • Herhangi Bir Güvenlik İhlalinde İhtiyaç Duyulacak Kayıt Bilgileri • Yasal veya Kurumsal Politikalara Uyumluluk için Toplanması Gereken Kayıtlar • Kayıt Toplanırken En Sık Yapılan Yanlışlar ve Karşılaşılan Sorunlar • Kayıt Toplanmasında Takip Edilebilecek Standartlar

1. ORACLE VERİTABANI GÜVENLİĞİ

Eğitimin Süresi	3 gün
Ön Şartlar	Veritabanları hakkında genel bilgi ve temel veritabanı yönetimi hakkında bilgi sahibi olmak.
Kimler Katılabilir?	• Veritabanı yöneticileri, • Veritabanı güvenlik denetleyicileri.
Eğitim Hedefleri	• Veritabanı güvenlik denetimi yapma kabiliyetinin edinimi, • Güvenli olarak veritabanı yönetme kabiliyetinin edinimi.
Konu Başlıkları	• Veritabanı Esasları • Kimlik Denetimi • Erişim Kontrol Listeleri • Veritabanı Güvenlik Denetlemesi • Ağ Güvenliği • Veritabanı Yedekleme • Erişim Araçlarının Denetlenmesi • İleri Düzey Güvenlik Önlemleri

2. MS SQL SERVER VERİTABANI GÜVENLİĞİ

Eğitimin Süresi	3 gün
Ön Şartlar	Veritabanları hakkında genel bilgi ve temel veritabanı yönetimi hakkında bilgi sahibi olmak.
Kimler Katılabilir?	• Veritabanı yöneticileri, • Veritabanı güvenlik denetleyicileri.
Eğitim Hedefleri	• SQL Server veritabanı güvenlik mekanizmaları ve güvenliğe etki eden kavramlar hakkında bilgi edinimi, • SQL Server güvenlik denetimi kabiliyetinin edinimi, • Güvenli olarak veritabanı yönetme yeteneğinin kazanımı.
Konu Başlıkları	• SQL Server, Genel Konular • İşletim Sistemi Yapılandırması • Ağ Konfigürasyonu • SQL Server Kurulumu ve Güncellemeler • SQL Server Ayarlarının Yapılması • Erişim Kontrolü ve Yetkilendirmeler • Denetleme ve Kayıt Altına Alma İşlemleri • Yedek Alma ve Felaketten Kurtarma Prosedürleri • Replikasyon • Yazılım Geliştirme Konuları • “Surface Area Configuration” Aracı • SQL Server Test ve İzleme Araçları

3. WEB UYGULAMALARI GÜVENLİĞİ

Eğitimin Süresi	2 gün
Ön Şartlar	Web teknolojileri hakkında temel bilgiler (HTTP, HTML, web sunucuları, internet tarayıcıları) ve uygulamalarda kullanılan dillerden en az birisini bilmek (PHP, Java, ASP.NET, Perl, v.b.).
Kimler Katılabilir?	• HTTP tabanlı uygulama geliştiricileri ve denetleyicileri.
Eğitim Hedefleri	• HTTP tabanlı uygulamaların önemli güvenlik bileşenleri, en çok yapılan güvenlik hataları, bu hataların nasıl giderileceği ve sürdürülebilir uygulama güvenliğin sağlanması hakkında bilgi edinimi.
Konu Başlıkları	• Bilgi Toplama • Ayar Yönetimi • Kimlik Doğrulama • Girdi/Çıktı Denetimi • Oturum Yönetimi • Yetkilendirme • Uygulama Mantığı • Kayıt Tutma • Hata Yönetimi • Güvenli Uygulama Yönetimi

SGE
GELİŞMİŞ SEVİYE EĞİTİMLER

4. MERKEZİ GÜVENLİK KAYIT YÖNETİM SİSTEMLERİ

Eğitimin Süresi	4 gün
Ön Şartlar	Bilgi sistemi bileşenlerinden haberdar olma, BT sistemleri içinde kullanılan güvenlik bileşenleri hakkında genel bilgi sahibi olmak.
Kimler Katılabilir?	• Bilgi sistemi yöneticileri, • Bilgi sistemi güvenlik yöneticileri, • BT denetim sorumluları.
Eğitim Hedefleri	• Merkezi saldırı ilişkilendirme sistemleri konusunda bilgi edinimi, • BT sistemlerinde bulunan farklı güvenlik bileşenlerinde oluşan kayıtları merkezi olarak toplama yeteneğinin kazanımı, • BT sistemlerine içeriden veya dışarıdan yapılan saldırıları merkezi olarak izleme ve önlem alma kabiliyetinin kazanımı.
Konu Başlıkları	• Merkezi Kayıt Yönetim Sistemleri • Olay İlişkilendirme Sistemlerine Duyulan İhtiyaç • Olay İlişkilendirme Adımları • Olay İlişkilendirme Sistemlerinin Faydaları • OSSIM Saldırı İlişkilendirme Sistemi • OSSIM Tanıtım • OSSIM Temel Bileşenleri • OSSIM'de Kullanılan Araçlar • OSSIM Kurulumu • OSSIM Bileşen Konfigürasyonu • Politikalar • Farklı Bileşenlerden Bilgi Toplama • Saldırı İlişkilendirme • Sistem Bakımı ve Güncelleme

5. SIZMA TESTİ UZMANLIĞI

Eğitimin Süresi	5 gün
Ön Şartlar	Güvenlik bilincine ve güvenlik alanında tecrübeye sahip olmak, orta seviyede Linux, Windows ve TCP/IP bilgisine sahip olmak, bilgi sistemleri altyapısında orta derecede deneyim sahibi olmak.
Kimler Katılabilir?	• Sızma testi ve güvenlik denetimlerinde görev alacak personel, • Bilgi güvenliği birimlerinde çalışan personel.
Eğitim Hedefleri	• Sızma testi yapma kabiliyetinin kazanımı.
Konu Başlıkları	• Giriş (Sızma testi nedir? Sızma testi öncesinde, sızma testi sırasında ve sızma testinden sonra dikkat edilecek hususlar, sızma testi metodolojileri) • Keşif (Keşif türleri, uygulamalı nmap kullanımı, keşif, port taraması, servis tespiti, işletim sistemi tespiti vb.) • Zafiyet tespiti (Zafiyet kavramı, Nessus kullanımı, politika oluşturma, tarama ve zafiyetlerin incelenmesi) • Exploit (Exploit ve payload kavramları, Metasploit kullanımı, msfconsole, meterpreter, post-exploit ve auxiliary modülleri vb.) • Dış Ağ Testleri ve Bilgi Toplama (Aktif ve pasif bilgi toplama, “Google hacking” vb.) • Sosyal Mühendislik (Telefon ve e-posta yolu ile sosyal mühendislik teknikleri, SET kullanımı, Özelleştirilmiş payload ve zararlı kod oluşturma - makro, pdf, exe. “Relay” zafiyeti, “Post-exploitation”) • Web Uygulamaları Testleri (Girdi-çıktı alanları tespiti, XSS ve SQL-i saldırıları)

6. KAYIT ANALİZİ

Eğitimin Süresi	5 gün
Ön Şartlar	Temel işletim sistemleri, veritabanı sistemleri ve ağ bilgisine sahip olmak.
Kimler Katılabilir?	• Sistem, güvenlik ve ağ yöneticileri, • Bilgi ve bilişim sistemleri uzmanları, • Bilgi güvenliği yöneticileri ve uzmanları.
Eğitim Hedefleri	• Kayıt (log) ve kayıt tutma ile ilgili temel bilgilerin edinimi, • Olay müdahalede kayıt yönetimi ve analizi yeteneğinin kazanımı, • Hangi kayıt çeşidinin hangi durumlarda ve olay müdahalenin hangi aşamasında kullanılacağı tecrübesinin kazanımı, • Kayıt analizi için temel analiz kabiliyetlerin kazanımı, • Kayıt toplama araçları hakkında genel bilgi ve beceri edinimi ve farklı kayıt analiz araçlarını kullanma yetkinliğinin kazanımı.
Konu Başlıkları	• Kayıt Analizi Genel Bakış Açısı • Kayıt Analizi Standartları, Kurallar ve Yasal Düzenlemeler • Kayıt Tutma, Kayıt Toplama, Görüntüleme Araçları • Kayıt Analizinde Yapılan Genel Hatalar • Olay Müdahale Çalışmaları • Olay Müdahalenin Farklı Aşamalarında Kayıt Kullanımı • Farklı Kaynaklardan Elde Edilen Kayıtların Olay Müdahale ve Analizlere Katkısı

7. DDoS SALDIRILARI İLE MÜCADELE

Eğitimin Süresi	2 gün
Ön Şartlar	Temel seviyede TCP/IP bilgisine, temel seviyede ağ ve aktif cihaz yönetim bilgisine sahip olmak.
Kimler Katılabilir?	• Sistem ve ağ yöneticileri.
Eğitim Hedefleri	• Ağ trafiğini kaydetme ve temel seviyede inceleme kabiliyetinin kazanımı, • DoS/DDoS saldırıları ve çeşitleri hakkında bilgi edinimi, • DoS/DDoS saldırılarından korunma yöntemleri hakkında bilgi edinimi.
Konu Başlıkları	• Bilgi Güvenliği • DoS/DDoS Saldırıları ve Çeşitleri • DoS/DDoS Saldırılarından Korunma Yöntemleri

8. MOBİL GÜVENLİK

Eğitimin Süresi	5 gün
Ön Şartlar	• IP, HTTP, TCP, UDP, vb. ağ protokolleri, Wireshark vb. ağ dinleme araçları hakkında giriş seviyesinde bilgi sahibi olmak, temel seviyede *NIX türevi işletim sistemlerini kullanabilmek, temel güvenlik konseptleri ve sızma testi hakkında bilgi sahibi olmak, mobil uygulama geliştirme hakkında temel seviyede bilgi sahibi olmak, okuduğu kod parçasını anlayabilmek.
Kimler Katılabilir?	• Mobil uygulama güvenliği sızma testi ve mobil zararlı yazılım analizi yapmak isteyen bilişim teknolojileri çalışanları.
Eğitim Hedefleri	• Eğitime katılanlar iOS ve Android işletim sistemi platformlarının sunmuş olduğu güvenlik özellikleri konusunda bilgi edinecekler, mobil uygulama sızma testi yapabilme kabiliyeti kazanacaklardır. Buna ek olarak, mobil zararlı yazılım analiz edebilme yeteneğine sahip olacaklardır. Not: iOS uygulamalarına yönelik pratik uygulamaların gerçekleştirilebilmesi için katılımcıların Jailbreak yapılmış bir iOS cihaza (iPhone, iPad, iPod) sahip olmaları gerekmektedir. Katılımcılara eğitmen tarafından herhangi bir cihaz temin edilmeyecektir.
Konu Başlıkları	• Mobil Güvenlikte Temel Kavramlar • Android İşletim Sistemi Temelleri • Android İşletim Sistemi Güvenlik Özellikleri • Android Uygulama Sızma Testi • iOS İşletim Sistemi Temelleri • iOS İşletim Sistemi Güvenlik Özellikleri • iOS Uygulama Sızma Testi • Mobil Zararlı Yazılımlar ve Analizi

1. TEMEL BİLGİSAYAR ANALİZİ

Eğitimin Süresi	3 gün
Ön Şartlar	Temel Linux ve Windows işletim sistemi bilgisine sahip olmak.
Kimler Katılabilir?	• Bilgisayar analizi yapmak isteyen bilgi sistem personeli.
Eğitim Hedefleri	• Bilgisayar analizi yapma kabiliyetinin kazanımı.
Konu Başlıkları	• Bilgisayar Olaylarına Müdahale • İşletim Sistemlerinde Dosyalama Sistemleri (NTFS, FAT32, ext2, ext3) Hakkında Bilgiler (Dosyaların bu sistemlerde ne şekilde oluşturulduğu, saklandığı, silindiği vb.) • Bilgisayarların Çeşitli Bölümleri için (RAM, "Stack" Alanı, sabit diskler vb.) Verilerin Kalıcılığı ve Veri Çıkarma Şekilleri • Linux Üzerinde Bilgisayar Olayı Analizi Yapılması ve İlgili Araçların Tanıtımı • Uygulamalı Kısımda Analiz Çalışma Ortamının Kurulması ve Araçlarla Şüpheli Dosya İncelemesi Yapılması • Windows Üzerinde Bilgisayar Olayı Analizi Yapılması ve İlgili Araçların Tanıtımı

2. AĞ TRAFİK ANALİZİ

Eğitimin Süresi	4 gün
Ön Şartlar	Temel TCP/IP ve ağ bilgisi, Temel Linux ve Windows işletim sistemi bilgisine sahip olmak.
Kimler Katılabilir?	• Ağ, sistem ve güvenlik yöneticileri, • Bilgisayar ağları analizi yapmak isteyen bilgi sistem personeli.
Eğitim Hedefleri	• Siber suçlarda olay analizi ve delil toplama süreçlerini hafıza birimlerine erişmeden gerçekleştirme yeteneğinin kazanımı, • Ağ bileşenlerinden kaynaklanan hataları ve zararlı ağ trafiğini tespit etme kabiliyetinin kazanımı.
Konu Başlıkları	• Ağ Paketi Yakalama Teknolojileri: Donanımlar, Yazılımlar ve Araçlar • Temel Ağ Protokolleri ve Bileşenleri • Ağ Güvenliği Bileşenleri Kayıt Dosyası Analizi: Güvenlik Duvarı, Saldırı Tespit ve Önleme Sistemi vb. Sistemlerin Kayıt Dosyaları • Ağ Protokollerinin Analizi. (HTTP, SMTP, DNS vb. protokoller için) • Derinlemesine Ağ Paketi Analizi • Zararlı Ağ Trafiğinin Tespit Edilmesi: “Araya Girme Saldırısı”, “DNS Önbellek Zehirlenmesi” vb. Saldırılar • Ağ Trafiği Tünelleme Tekniklerinin Tespit Edilmesi: DNS, ICMP, SSH Tünelleme vb. Teknikler • Şifreli Ağ Trafiğinin Analizi: “SSL Trafiği Dinleme” Tekniği • Ağ Trafiğinin Yeniden İnşa Edilerek Orijinal Verilerin Elde Edilmesi • Ağ Akış Analizi

3. WINDOWS ZARARLI YAZILIMLARI ANALİZİ

Eğitimin Süresi	5 gün
Ön Şartlar	Değişkenler, döngüler ve fonksiyonlar gibi yüksek seviye programlama kavramlarını tanımak, Windows işletim sisteminin (“process”, “thread”, “memory management”, “registry”, “handle” vb.) temel kavramları hakkında bilgi sahibi olmak, IP, HTTP, TCP, UDP, vb. ağ protokolleri, Wireshark vb. ağ dinleme araçları hakkında giriş seviyesinde bilgi sahibi olmak, Assembly ve x86 mimarisi hakkında giriş seviyesinde bilgi sahibi olmak.
Kimler Katılabilir?	• Zararlı yazılım incelemesi yapmak isteyen bilişim teknolojileri çalışanları.
Eğitim Hedefleri	• Tersine mühendislik konusunda pratiğe yönelik bilgi edinimi, • Windows ve web tabanlı zararlı yazılımlar ile zararlı dokümanları analiz kabiliyetinin kazanımı.
Konu Başlıkları	• Windows İşletim Sistemi, Temel Kavramlar • Basit Statik Analiz • Davranış Analizi • Kod Analizi • Gizli Çalışma Yöntemleri • Statik Analiz Engelleme Yöntemleri • Dinamik Analiz Engelleme Yöntemleri • Paketlenmiş Yazılımların Paketten Çıkarılması • Bellek Dokümü Analizi • Web (Tarayıcı) Tabanlı Zararlı Yazılımların Analizi • Zararlı Dokümanların Analizi

4. GÜVENLİ YAZILIM GELİŞTİRME

Eğitimin Süresi	3 gün
Ön Şartlar	Yazılım dillerinden herhangi birine orta seviyede hakim olmak.
Kimler Katılabilir?	• Yazılım geliştiricileri/mühendisleri, • Yazılım projesi yöneticileri, • Yazılım kalite kontrol ekibi, • Sistem mimarları.
Eğitim Hedefleri	• Temel güvenli kodlama prensipleri, güvenli yazılım tasarımı, tehdit modellemesi, güvenli yazılım geliştirme ve güvenlik öncelikli test prensipleri hakkında bilgi edinimi.
Konu Başlıkları	• Yazılım ve Yazılımın Koştuğu Teknoloji Bileşenlerinin Güvenlik Problemleri • Güvenli Yazılım Geliştirme Sürecinin Temel Öğeleri ve Güvenli Yazılım Geliştirme Yaşam Döngüsünün Yazılım Geliştirme Sürecine Nasıl Entegre Edileceği • Sürece Ek Olarak Kaynak Kod Örnekleriyle En Çok Karşılaşılan Zafiyetler ve Bu Zafiyetlerin Nasıl Önlenebileceği • Yazılımın Sadece Koddan İbaret Olmadığı Varsayımıyla Yazılımın Üzerinde Koştuğu Uygulama Sunumcu, Veri Tabanı Gibi Bileşenlerin Güvenli Çalışması için Kullanılabilecek Teknolojiler

5. İLERİ SIZMA TESTİ UZMANLIĞI

Eğitimin Süresi	5 gün
Ön Şartlar	Sızma testi uzmanlığı eğitimini almış olmak, orta seviyede Linux, Windows ve TCP/IP bilgisine sahip olmak, temel seviyede programlama tecrübesine (Betik dilleri) sahip olmak.
Kimler Katılabilir?	• Sızma testi ve güvenlik denetimlerinde görev alacak personel.
Eğitim Hedefleri	• Sızma testlerinde ileri seviye saldırı tekniklerini kullanma yetkinliğinin kazanımı.
Konu Başlıkları	• Ağ Paketi Üretme (Scapy) • Etki Alanı Testleri (mimikatz, metasploit modülleri, meterpreter modülleri, incognito, remote registry, golden ticket, pivoting) • Araya Girme Saldırıları (ARP spoof, SSL Strip, SMB redirect, fake SMB Auth, LLMNR poisoning, DHCP starvation, rogue DHCP server, DNS spoofing, Mimf, scapy snipets) • Parola Kırma Saldırıları (şifre - özet türleri, çevrimdışı parola kırma, john, cain, çevrimiçi parola kırma, hydra, gökküşağı tabloları, crunch, ophcrack, python betikleri) • Kablosuz Ağ Testleri (Ağı dinleme, de-authentication, araya girme, handshake yakalama, parola kırma saldırıları, şifreli trafiği çözme, wps pin kırma, rogue ap, radius sunucu saldırıları, scapy snipets) • Heartbleed, Shellshock

UEKAE EĞİTİMLERİ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

UEKAE

1. AKILLI KART İŞLETİM SİSTEMİ EĞİTİMİ

Eğitimin Süresi	2 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• AKİS üzerinde uygulama geliştirmek isteyenler, • AKİS yüklü kartlar ile çalışan bilgisayar uygulaması geliştirmek isteyenler.
Eğitim Hedefleri	• Akıllı kart işletim sistemleri ve genel özellikleri hakkında bilgi sahibi olunması, • AKİS üzerinde uygulama geliştirebilecek seviyede bilgi sahibi olunması, • AKİS yüklü kartlar ile çalışan sürücü yazılımı ve/veya kütüphane yazılımı geliştirebilecek düzeyde bilgi sahibi olunması.
Konu Başlıkları	• Akıllı Kartlar ve Kullanım Alanları • AKİS ve Uygulama Alanları • AKİS Haberleşme Protokolü • AKİS Yaşam Evreleri • AKİS Dosyalama Yapısı, Güvenlik Mimarisi ve Komutları • AKİS Bilgisayar Uygulamaları (PKCS11, PKCS15, CSP, mini sürücü)

2. KART ERİŞİM CİHAZI STANDARDI EĞİTİMİ

Eğitimin Süresi	2 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• TS 13582, TS13583, TS 13584, TS 13585 standartlarında tanımlı Kart Erişim Cihazı (KEC) geliştirmek isteyenler.
Eğitim Hedefleri	• Kart Erişim Cihazı (KEC) geliştirebilecek düzeyde bilgi sahibi olunması, • KEC'in sertifikasyon süreçleri hakkında bilgi sahibi olunması.
Konu Başlıkları	• Standardlar ile İlgili Temel Kavramlar • Elektronik Kimlik Doğrulama Sistemi (EKDS) • KEC Arayüzleri ve Özellikleri • KEC Uygulama Yazılımı Özellikleri • KEC Protokolleri • Türkiye Cumhuriyeti Kimlik Kartı ve EKDS Veri Yapıları ve Erişim Kuralları • KEC Ortak Kriterler (Common Criteria, CC) Sertifikasyon Süreci • KEC TSE Standardı Sertifikasyon Süreci

UEKAE

3. KART ERİŞİM CİHAZI ORTAK KRİTERLER SERTİFİKASYON EĞİTİMİ

Eğitimin Süresi	1 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• TS 13582, TS13583, TS 13584, TS 13585 standartlarında tanımlı Kart Erişim Cihazı (KEC) geliştirmek isteyenler.
Eğitim Hedefleri	• Kart Erişim Cihazının geliştirilmesi öncesinde Ortak Kriterler ve Kart Erişim Cihazı Koruma Profilinin getirdiği ürün gerekleri hakkında bilgi sahibi olunması ve güvence gereklerinden güvenlik hedefi dokümanının (ST) hazırlanabilmesi.
Konu Başlıkları	• Ortak Kriter (CC) Değerlendirme Süreci • Kart Erişim Cihazının (KEC) Tanımı • Kart Erişim Cihazı (KEC) Güvenlik Problem Tanımı • Kart Erişim Cihazı (KEC) Güvenlik Hedefleri • Kart Erişim Cihazı (KEC) Güvenlik İşlevsel Gerekleri • Kart Erişim Cihazı (KEC) Güvenlik Güvence Gerekleri

4. ELEKTRONİK KİMLİK DOĞRULAMA SİSTEMİ (EKDS) STANDARDI EĞİTİMİ

Eğitimin Süresi	2 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• TS 13678, TS 13679, TS 13680, TS 13681 standartlarında tanımlı Kimlik Doğrulama Sunucusu (KDS), Kimlik Doğrulama Politika Sunucusu (KDPS), Rol Doğrulama Sunucusu veya Kimlik Kartı Yazılım Kütüphanesi geliştirmek isteyenler.
Eğitim Hedefleri	• Elektronik Kimlik Doğrulama Sistemi (EKDS) bileşenleri olan Kimlik Doğrulama Sunucusu (KDS), Kimlik Doğrulama Politika Sunucusu (KDPS), Rol Doğrulama Sunucusu veya Kimlik Kartı Yazılım Kütüphanesi'ni geliştirebilecek düzeyde bilgi sahibi olunması.
Konu Başlıkları	• Elektronik Kimlik Doğrulama Sistemi (EKDS) • Kimlik Kartı Veri Yapıları ve Erişim Koşulları • Kimlik Kartı Yazılım Kütüphanesi • Kimlik Doğrulama Sunucusu (KDS) • Kimlik Doğrulama Politika Sunucusu (KDPS) • Kimlik Tanıma ve Doğrulama Yöntemleri • Rol Doğrulama ile Veri Erişimi

5. T.C. KİMLİK KARTI KULLANIM VAKALARI EĞİTİMİ

Eğitimin Süresi	1 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• İş süreçlerini T.C. Kimlik Kartı ve Elektronik Kimlik Doğrulama Sistemi'ne (EKDS) entegre etmek isteyen iş analistleri ve uygulama geliştiricileri.
Eğitim Hedefleri	• T.C. Kimlik Kartı, Elektronik Kimlik Doğrulama Sistemi (EKDS), Kimlik Tanıma ve Doğrulama Yöntemleri ve Kimlik Kartı Kullanım Vakaları konuları hakkında bilgi sahibi olunması.
Konu Başlıkları	• T.C. Kimlik Kartı Tanıtımı • T.C. Kimlik Kartı Görsel Güvenlik Özellikleri • Elektronik Kimlik Doğrulama Sistemi (EKDS) • Kimlik Tanıma ve Doğrulama Yöntemleri • Kimlik Kartı Kullanım Vakaları

YTE EĞİTİMLERİ

Yazılım Teknolojileri Araştırma Enstitüsü

EKRAN TASARIMI VE KULLANILABİLİRLİK EĞİTİMİ

Eğitimin Süresi	2 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• Tasarımcılar, • İş Analistleri, • Sistem Analistleri, • Yazılım/Uygulama geliştiriciler, • Test Mühendisleri.
Eğitim Hedefleri	• Ekran tasarımı konusunda bilgi sahibi olma, • Kullanılabilirlik ile ilgili temel kavramları ve yaklaşımları anlama, • Etkileşim türlerini ve görsel arayüz tasarımını anlama, • Evrensel tasarım ve erişilebilirlik hakkında bilgi sahibi olma, • Kullanılabilirlik değerlendirmelerini anlama,
Konu Başlıkları	• Kullanıcı Deneyimi Tasarımı • Kullanılabilirlik ve Kullanılabilirlik Mühendisliği • Kullanıcı Araştırması ve Persona • Bilgi Mimarisi ve Kart Sıralama • Prototiplendirme • Arayüz Tasarım Prensipleri • Evrensel Tasarım ve Erişilebilirlik • Kullanılabilirlik Testleri

Kamu SM EĞİTİMLERİ

Kamu Sertifikasyon Merkezi

1. TEMEL KRİPTOLOJİ VE BİLGİ GÜVENLİĞİ

Eğitimin Süresi	1 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• e-imza uygulamaları yazacak/yazdıracak kurum veya kuruluşlar, • Kurum/kuruluşlarda e-imza konusunda karar verici kişiler.
Eğitim Hedefleri	• Simetrik/Asimetrik algoritmalar hakkında bilgi edinme, • Özet algoritmalar hakkında bilgi edinme, • Elektronik ortamda imzalama ve imza doğrulama bilgisi edinme, • Elektronik ortamda şifreleme ve şifre çözme bilgisi edinme.
Konu Başlıkları	• Kriptoloji Nedir? • Elektronik Tehditler ve Güvenlik • Basit Şifreleme – Güvenli Şifreleme • Simetrik Kriptografi – Gizli Anahtarlı Sistemler • Asimetrik Kriptografi – Açık Anahtarlı Sistemler • e-İmza Nasıl Atılır?

2. AÇIK ANAHTAR ALTYAPISI (AAA)

Eğitimin Süresi	1 gün
Ön Şartlar	"Temel Kriptoloji ve Bilgi Güvenliği Eğitimi" almış olmak.
Kimler Katılabilir?	• E-imza uygulamaları yazacak/yazdıracak kurum veya kuruluşlar, • Kurum/kuruluşlarda e-imza konusunda karar verici kişiler.
Eğitim Hedefleri	• Elektronik sertifika hakkında bilgi edinme, • AAA gerekliliği hakkında bilgi edinme, • Elektronik sertifika kullananlar için AAA'nın neden vazgeçilmez olduğu hakkında bilgi edinme, • OCSP ve CRL hakkında bilgi edinme, • Zaman Damgası, SSL gibi AAA uygulamaları hakkında bilgi edinme.
Konu Başlıkları	• AAA Neden Gereklidir? • AAA sertifikaları (Elektronik Sertifika) • Sertifika Üretimi ve İptali • CRL • OCSP • AAA Uygulamaları (SSL, Zaman Damgası, KEP, Logon, VPN)

3. e-İMZA VERİ FORMATLARI

Eğitimin Süresi	0.5 gün
Ön Şartlar	"Temel Kriptoloji ve Bilgi Güvenliği" ve "Açık Anahtar Altyapısı" eğitimlerini almış olmak.
Kimler Katılabilir?	• Kurum/kuruluşlarda e-imza konusunda karar verici kişiler, • e-imza yazılımı geliştiren yazılımcılar.
Eğitim Hedefleri	• e-İmza veri formatları hakkında bilgi sahibi olmak.
Konu Başlıkları	• BES İmza Tipi • ES-T İmza Tipi • X-Long İmza Tipi • Archieve İmza Tipi

4. e-İMZA KULLANICI EĞİTİMİ

Eğitimin Süresi	0.5 gün
Ön Şartlar	Belirli bir ön şart bulunmamaktadır.
Kimler Katılabilir?	• e-imza kullanıcıları.
Eğitim Hedefleri	• e-imza hakkında genel bilgi edinme, • Elektronik bir dosyanın nasıl imzalandığı ve nasıl doğrulandığı hakkında bilgi edinme.
Konu Başlıkları	• e-imzanın Detaylı Tanımı ve Önemi • e-imza ile Bir Doküman Nasıl İmzalanır? • e-imzalı Bir Dokümanın İmzası Nasıl Doğrulanır? • Akıllı Kartın İçinde Neler Bulunur? • İmzalamada Açık (Public) ve Özel (Private) Anahtar Fonksiyonları • Nitelikli Elektronik Sertifika (NES) Nedir? • e-imza ile NES Farkı Nedir?

5. CAdES (CMS TABANLI İLERİ e-İMZA)

Eğitimin Süresi	3 gün
Ön Şartlar	"Temel Kriptoloji ve Bilgi Güvenliği", "Açık Anahtar Altyapısı" ve "e-imza Veri Formatları" eğitimlerini almış olmak.
Kimler Katılabilir?	• e-imza yazılımı geliştiren yazılımcılar.
Eğitim Hedefleri	• Katılımcıların TÜBİTAK CAdES kütüphanesinin detaylarını öğrenip, bunları yazılımlarına rahatlıkla entegre edebilecek yetkinlikte olmalarının sağlanması.
Konu Başlıkları	• Akıllı Kart Kütüphanesi Konfigürasyonu • Sertifika Deposu Kütüphanesi Konfigürasyonu • Sertifika Doğrulama Detayları ve Konfigürasyonu • CAdES İmza Tiplerinin Detayları ve Oluşturulması • CAdES İmza Tiplerinin Değiştirilmesi • CAdES İmza Doğrulama Detayları ve Konfigürasyonu

6. XAdES (XML TABANLI İLERİ e-İMZA)

Eğitimin Süresi	2 gün
Ön Şartlar	"Temel Kriptoloji ve Bilgi Güvenliği", "Açık Anahtar Altyapısı", "e-imza Veri Formatları" ve "CAdES (CMS Tabanlı İleri e-İmza)" eğitimlerini almış olmak.
Kimler Katılabilir?	• e-imza yazılımı geliştiren yazılımcılar.
Eğitim Hedefleri	• Katılımcıların TÜBİTAK XAdES kütüphanesinin detaylarını öğrenip, bunları yazılımlarına rahatlıkla entegre edebilecek yetkinlikte olmalarının sağlanması.
Konu Başlıkları	• XAdES İmza Tiplerinin Detayları ve Oluşturulması • XAdES İmza Tiplerinin Değiştirilmesi • XAdES İmza Doğrulama Detayları ve Konfigürasyonu

Eğitim Kataloğu

2018-01

TÜBİTAK BİLGEM
T: 0262 648 1000 • F: 0262 648 1100 • E: bilgem@tubitak.gov.tr
W: www.bilgem.tubitak.gov.tr • A: PK.: 74, 41470, Gebze / Kocaeli