Co-funded by the European Union

D3.1 YÜKSEKÖĞRETIM ÖĞRENCILERI IÇIN EĞITIM MODÜLLERI

CYBER AGENT 09.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

www.cyberagents.eu

İş Paketi 3: CyberAgent Learning kaynak geliştirme

Çıktı 3.1: HEI öğrencileri için eğitim modülleri

WP3 Lideri – TIMTAL. D3.1 – VU'nun lideri.

İÇERİK

GIRIŞ

D2.2 raporuna göre, KOBİ'ler nitelikli siber güvenlik uzmanları konusunda önemli bir eksiklikle karşı karşıyadır ve mevcut çalışanlar genellikle giderek daha karmaşık hale gelen siber tehditlere uygun şekilde yanıt vermek için gereken sistemik bilgiden yoksundur. Bu nedenle, yüksek öğrenimde, bilgilerini KOBİ ortamında hem teknik hem de yönetimsel alanlarda uygulayabilecek uzmanlar hazırlamak özellikle önemlidir. Bunun ışığında, D2.3 belgesinde farklı tematik alanlara bölünmüş ve pratik becerilerin geliştirilmesine odaklanan yetkinlik temelli bir öğrenme yolu oluşturulmuştur.

Bu belge, ana proje çıktılarından birini sunar - yüksek öğrenim (HEI) öğrencileri için eğitim modülleri (D3.1). Bu faaliyetin amacı, küçük ve orta ölçekli işletmelerle (KOBİ'ler) ilgili siber güvenlik bilgi, beceri ve yeterliliklerinin temel alanlarını kapsayan yükseköğretim kurumları (HEI) için eğitim müfredatları oluşturmaktır.

Bu modüller, KOBİ'lerden, mesleki eğitim ve öğretimden (VET) ve yükseköğretim kurumlarından temsilcilerin ankete tabi tutulduğu ayrıntılı bir ihtiyaç analizine (D2.2) ve açıkça tanımlanmış bir öğrenme yolu yapısına (D2.3) dayalı tutarlı bir çalışmanın sonucudur.

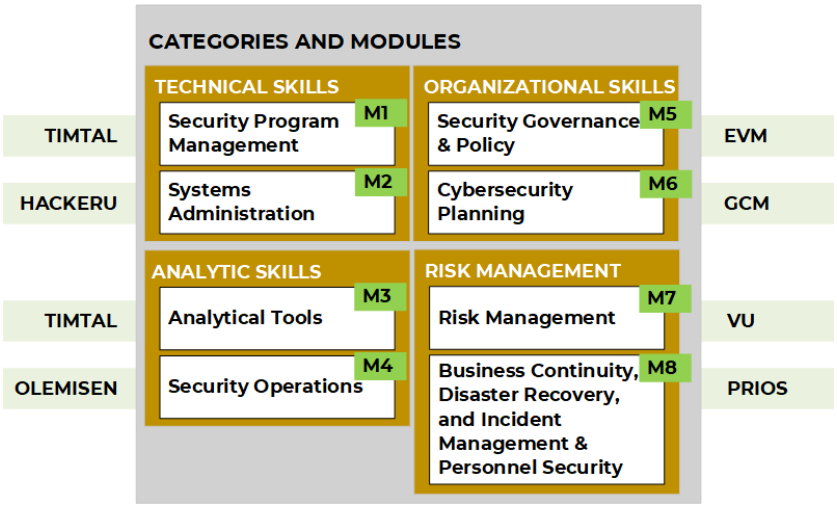
Avrupa Yeterlilikler Çerçevesi (AYÇ) 5-6 seviyelerine karşılık gelen eğitim programı, yükseköğretim öğrencileri ve ileri düzey KOBİ çalışanları için tasarlanmıştır. Dört temel yetkinlik alanını kapsayan sekiz temel modül ve bir ilham verici modülden oluşur:

- **Teknik Beceriler** (Güvenlik Programı Yönetimi, Sistem Yönetimi).
- **Analitik Beceriler** (Analitik Araçlar, Güvenlik Operasyonları).
- **Organizasyon Becerileri** (Güvenlik Yönetimi ve Politikası, Siber Güvenlik Planlaması).
- **Risk Yönetimi** (Risk Yönetimi ve Azaltma, İş Sürekliliği, Felaket Kurtarma ve Olay Yönetimi & Personel Güvenliği).

Her modül 3 AKTS kredisi değerindedir (75 saatlik öğrenci iş yüküne karşılık gelir), Yükseköğretim Alanı ilkeleriyle uyumludur ve D2.3'te belirtilen metodolojik önerilere bağlıdır: eğitim, aktif öğrenme yöntemlerine (örneğin, vaka çalışmaları, proje tabanlı öğrenme) ve kendi kendine öğrenmeye dayalıdır ve öğrenme çıktıları bilgi düzeylerinde açıkça ayırt edilir, beceriler ve yetkinlikler.

Her 3 AKTS'lik kredi modülü, farklı konsorsiyum ortakları tarafından, kendi alanlarından ve mesleki deneyimlerinden yararlanılarak geliştirilmiştir.

Geliştirilen modüller, D2.2 raporunda kritik öneme sahip olarak tanımlanan aşağıdaki temel alanları kapsamaktadır:



1. M1: GÜVENLIK PROGRAMI YÖNETIMI

Modül başlığı	Modül kodu
GÜVENLİK PROGRAMI YÖNETİMİ	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman

Dersin veriliş şekli	Dil
Yüz yüze, çevrimiçi, hibrit	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
Hiç kimse

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	75 saat	50 saat	25 saat

Modülün amacı ve sonuçları

Bu dersi bitirdikten sonra öğrenciler, siber güvenlik tehditlerine yanıt olarak güvenlik programlarını etkin bir şekilde yönetme becerileriyle donatılacaktır. Oltalama, fidye yazılımı ve DDoS saldırıları gibi güncel tehditlere karşı proje ve kaynak yönetimi çerçevesinde savunma stratejileri geliştireceklerdir. Ayrıca öğrenciler, güvenlik ölçümlerini ve kalite güvence yöntemlerini uygulamayı öğrenecek, güvenlik programlarını optimize etme, kaynakları verimli bir şekilde yönetme ve gelişen tehditlere karşı uygun araçları kullanarak kurumsal güvenliği artırma becerisi kazanacaklardır. Bu kurs aynı zamanda tehdit değerlendirmesi, raporlama ve iletişim konularında yetkinliklerini geliştirecek ve siber güvenlik stratejilerini kuruluşlarında etkili bir şekilde uygulamalarını sağlayacaktır.

Modülün öğrenme çıktıları	Öğretim ve öğrenme yöntemleri	Değerlendirme yöntemleri
Bilgi: Öğrenciler, kimlik avı, fidye yazılımı ve DDoS saldırıları dahil olmak üzere en son siber güvenlik tehditleri ve bunların etkili proje ve kaynak yönetimi ve kalite güvence ve kontrol önlemlerinin uygulanması yoluyla nasıl yönetileceği hakkında pratik bilgiler edineceklerdir.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. [Öğretim Yöntemleri, örneğin teorik dersler, konuk konuşmacılar, sınavlar, oyunlar, pratik görevler/laboratuvarlar, akranlar arası öğretme ve öğrenme, kendi kendine öğrenme vb.] D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı"	Öz değerlendirme testleri Bilgi değerlendirme testi

Beceriler: Öğrenciler, gelişen siber tehditlere karşı korunmak için araç ve yazılımları kullanma becerisine sahip olacak ve kuruluşlarındaki genel güvenlik ölçümlerini ve kalite kontrolünü geliştirmek için proje ve kaynak yönetiminde sağlam güvenlik uygulamaları uygulayacaktır.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. [Öğretim Yöntemleri, örneğin pratik görevler/laboratuvarlar, uygulamalı etkinlikler, simüle edilmiş ortamlar, sınavlar, oyunlar, vaka çalışmaları vb.] D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı"	Pratik değerlendirmeler
Yeterlilikler: Öğrenciler, potansiyel güvenlik tehditlerini değerlendirme ve azaltma, siber güvenlik sorunlarını etkili bir şekilde iletme ve tehditleri ve ihlalleri kuruluşlarındaki uygun kanallar aracılığıyla doğru bir şekilde raporlama konusunda yetkin olacaklardır.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. [Öğretim Yöntemleri, örn. simüle edilmiş ortamlar, bayrak yarışmalarını ele geçirme, 5E'ler, CBL, CL, POGIL, PBL vb.] D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı"	Simülasyon Yarışma

Modül içeriği: konuların dökümü	**İletişim çalışma saatleri**					**Bireysel çalışma saatleri ve görevler**	
	Dersler (HEI)	Danışma	Uygulama (HEI)	Test	**Tüm iletişim**	**Bireysel**	**Görev**
Proje yönetimi • Proje Planlaması • Proje Hedeflerinin Tanımlanması • Proje Kapsamının ve Gereksinimlerinin Tanımlanması • Proje Takviminin Hazırlanması • Proje Yönetim Araçları • Güncel Siber Güvenlik Tehditleri (DDoS, Ransomware, Kötü Amaçlı Yazılım, Phishing, Zero-Day, IoT saldırıları vb.) • Tehdit Modelleme ve Zafiyet Analizi • Acil Durum ve Olay Müdahale Planları • Siber Güvenlik Tehditlerini ve Olaylarını Raporlama	8	0,5	3	0,5	**12**	**6**	• KOBİ çalışanları için bir siber güvenlik farkındalık projesi planlayın. • KOBİ çalışanlarının potansiyel güvenlik tehditlerini anlamalarını geliştirmek için siber güvenlik farkındalık projesi için net hedefler tanımlayın. • Eğitim konuları ve gerekli kaynaklar da dahil olmak üzere KOBİ çalışanlarına yönelik siber güvenlik farkındalık projesinin kapsamını ve gerekliliklerini ana hatlarıyla belirtin. • KOBİ çalışanları için siber güvenlik farkındalık

							projesi için zaman çizelgesini hazırlayın. • KOBİ çalışanlarına yönelik siber güvenlik farkındalık projesinin ilerlemesini ve kaynak kullanımını izlemek için proje yönetimi araçlarını kullanın. • Mevcut siber güvenlik tehditlerini araştırın ve bulguları bir rapor halinde derleyin. • KOBİ çalışanlarının günlük operasyonlarındaki potansiyel güvenlik açıklarını belirlemelerine yardımcı olmak için basitleştirilmiş bir tehdit modeli oluşturun. • Acil durum ve olay müdahale planı örneklerini bulun ve inceleyin. • Siber güvenlik tehditlerinin ve olaylarının raporlanmasına ilişkin rapor hazırlarken hangi adımlar dikkate alınmalıdır? Araştırın ve özetleyin.
Kaynak yönetimi • İnsan Kaynakları (Proje Ekipleri) Yönetimi • Güvenlik Farkındalığı ve Ekip Eğitimi • Donanım ve Yazılım Envanter Yönetimi • Güvenlik Araçları ve Yazılımları • Teknolojik Kaynakların Etkin Kullanımı • Bütçe ve Kaynak Tahsisi	8	0,5	3	0,5	**12**	**6**	• Kurgusal bir KOBİ için kaynakların etkin kullanımını sağlamak için bir kaynak yönetimi stratejisi planlayın. • Siber güvenlik farkındalığı eğitimi için örnek bir konu planı oluşturun. • Kurgusal bir KOBİ için donanım ve yazılım envanteri hazırlayın. • Yaygın olarak kullanılan güvenlik araçlarını ve yazılımlarını araştırın. • Varsayımsal bir KOBİ için örnek bir bütçe ve kaynak tahsis planı oluşturun.

Güvenlik ölçümleri • Güvenlik Metrikleri ve Ölçüm Teknikleri • SIEM ile Veri Toplama • Güvenlik Metriklerinin Analizi • Proje İzleme ve Performans Değerlendirme • Aksiyonların Gözden Geçirilmesi ve Proje Uyarlaması • Güvenlik Metriklerinin Raporlanması	8	0,5	4	0,5	**13**	**6**	• KOBİ'lerde siber güvenlik duruşunu değerlendirmek için kullanılan güvenlik ölçümlerini araştırın. • SIEM yazılımının günlükleri topladığı kaynakları araştırın. • Açık kaynaklı bir SIEM yazılımı kurun ve inceleyin. • SIEM yazılımını kullanarak günlükleri toplayarak güvenlik ölçümlerini analiz edin. • Güvenlik metriklerinin analiz sonuçlarını grafik ve görsellerle raporlayın.
Kalite güvencesi ve kalite kontrol • Kalite Yönetimi • Siber Güvenlikte Kalite Standartları • Uygunluk ve Kalite Denetimleri • Test ve Doğrulama Teknikleri • Değerlendirme ve İyileştirme Önerileri	8	0,5	4	0,5	**13**	**7**	• KOBİ'lerde siber güvenlik uygulamalarının etkinliğini artırmak için kalite güvence ve kalite kontrol süreçleri nasıl planlanmalıdır? Araştırın ve özetleyin. • ISO/IEC 27001:2022'nin Ek A Kontrol Öğelerini araştırın. • Test ve doğrulama tekniklerinin ne olduğunu araştırın ve raporlayın. • Kalite süreçlerinin sürekli gözden geçirilmesi ve iyileştirilmesi KOBİ'lere ne gibi faydalar sağlar?
Toplam	**32**	**2**	**14**	**2**	**50**	**25**	

Değerlendirme stratejisi	**Karşılaştırmalı ağırlık yüzdesi**	**Değerlendirme kriterleri**
Öz değerlendirme testi I	10%	10 puan - %95-100 doğru cevap. 9 puan – %85-94 doğru cevap. 8 puan – %75-84 doğru cevap. 7 puan - %65-74 doğru cevap. 6 puan – %55-64 doğru cevap. 5 puan – %45-54 doğru cevap. 4 puan – %35-44 doğru cevap. 3 puan – %25-34 doğru cevap.
Öz değerlendirme testi II	10%	
Öz değerlendirme testi III	10%	
Öz değerlendirme testi IV	10%	
Bilgi değerlendirme testi	60%	

2 puan – %15-24 doğru cevap.
1 puan – %0-14 doğru cevap.

Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*
Gerekli okuma
Önerilen kaynaklar
https://sansorg.egnyte.com/dl/RFrVIbX2oc https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf https://healthybyte.net/cybersecurity/what-is-a-security-program-management

2. M2: SISTEM YÖNETIMI

Modül başlığı	Modül kodu
SİSTEM YÖNETİMİ	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman

Dersin veriliş şekli	Dil
Yüz yüze, çevrimiçi, karma	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
Hiç kimse

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	75	50	25

Modülün amacı ve sonuçları

Bu dersi bitirdikten sonra öğrenciler, risk analizi, değerlendirme ve tedaviyi planlayarak, uygulayarak, raporlayarak ve ileterek BİT altyapılarının, sistemlerinin ve hizmetlerinin siber güvenlikle ilgili risklerini sürekli olarak yönetebileceklerdir (tanımlama, analiz etme, değerlendirme, tahmin etme, azaltma). Öğrenciler, ağ cihazlarını düzgün bir şekilde yönetmek, hem Linux hem de Windows sunucularında çalışmak ve güvenliğini sağlamak için Ağ temellerini bileceklerdir. Ayrıca siber güvenlik bağlamında Bulut ve Yapay Zeka hakkında bilgi sahibi olmak, görevleri düzgün bir şekilde hızlandırmak, otomasyonları ve ölçeklendirmeyi gerçekleştirmek için çok faydalı olacaktır. Öğrenciler ayrıca sistemleri nasıl güçlendireceklerini, tehdit avcılığı yapmayı ve sunucuları nasıl kullanılabilir hale getireceklerini öğreneceklerdir (CIA üçlüsünün kısaltması).

Modülün öğrenme çıktıları	Öğretim ve öğrenme yöntemleri	Değerlendirme yöntemleri
Bilgi: Öğrenciler Ağ Yönetimi, İşletim Sistemleri, Ağ Temelleri, Ağ Yönetim Araçları, Ağ cihazları güvenliği, Linux Sistem Yönetimi, Windows Sistem Yönetimi, Sanallaştırma, Ağ ve siber güvenlik prosedürleri için yapay zeka kullanarak Bulut Bilişim, Siber Güvenlik Prosedürleri, Tehdit Tespiti, Tehdit Analizi, Tehdit Yanıtı, Tehdit Düzeltme, Siber Güvenlik Temelleri, Kuruluşu saldırılara karşı savunma, Altyapı & Ağ Güvenliği, Ağ İzleme & Analiz, Olay İşleme. Uyum standartlarında KOBİ işyerlerinin özel ihtiyaçlarına göre uyarlanmış etkili sistem yönetimi prosedürleri, operasyonel rutinler oluşturabilecek ve tanımlayabileceklerdir.	Öğretim üyesi tarafından seçilecek, canlı dersler, video kayıtları, sunumlar, sanal cihazlar (varsa), literatür analizi, konuk konuşmacılar, akranlar arası öğretme ve öğrenme, mentorluk.	Öz değerlendirme testleri ve bilgi değerlendirme testleri
Beceriler: Öğrenciler, KOBİ işyerleri için işletim sistemleri, veritabanları, ağlar ve bulut altyapıları dahil olmak üzere güvenli sistem mimarilerini tasarlamak ve uygulamak için metodolojileri ve araçları kullanma becerisine sahip olacaklardır.	Öğretim üyesi tarafından seçilecek, canlı dersler, video kayıtları, sunumlar, sanal cihazlar (varsa), literatür analizi, konuk konuşmacılar, akranlar arası öğretme ve öğrenme, mentorluk.	Öz değerlendirme testleri ve bilgi değerlendirme testleri

Yetkinlikler: Öğrenciler, sistem yönetimi için stratejik siber güvenlik çerçeveleri geliştirme ve uygulama, sistem güçlendirme ve kullanılabilirliğini artırmak için projelere ve ekiplere liderlik etme ve KOBİ işyerleri için çeşitli idari alanlarda sağlam siber güvenlik uygulamalarını sürdürme konusunda etik kararlar alma konusunda yetkin olacaklardır.	Öğretim üyesi tarafından seçilecek, canlı dersler, video kayıtları, sunumlar, sanal cihazlar (varsa), literatür analizi, konuk konuşmacılar, akranlar arası öğretme ve öğrenme, mentorluk.	Öz değerlendirme testleri ve bilgi değerlendirme testleri

Modül içeriği: konuların dökümü	**İletişim çalışma saatleri**					**Bireysel çalışma saatleri ve görevler**	
	Dersler (HEI)	Danışma	Uygulama (HEI)	Test	**Tüm iletişim**	**Bireysel çalışma**	**Görev**
İşletim sistemi yönetimi • İşletim Sistemleri • Donanım ve Yazılım Arasındaki İlişki • İkililer, Onaltılık Sayma • Bitler & Baytlar • İşletim sisteminde komut satırı • Windows & Linux Komutları • Windows İstemci & Sunucu • Windows'ta Uygulamalar, İşlemler ve Hizmetler • Dosya Uzantıları & Türleri • Kayıt Defteri Anahtarları ve Değerleri • Kontrol Paneli Ayarları • Kullanıcılar ve Gruplar • Domain Yapısı & Sunucu Yöneticisi • AD & GPO • Linux Arayüzleri & Çekirdek • Linux'ta Süreçler • Dosya & Dizin Adlandırma Kuralları • Linux Kabukları & Komut Sözdizimi • Dosya & Klasörleri Manipüle Etme • Boru & Sistem İzleme Komutları ile Çalışma	4	0,5	2	0,5	**7**	**3,5**	Onaltılık Sayma Windows Komutlarını Uygulama Linux Komutlarını Uygulama Görev Yöneticisini Uygulamak Dosyaların oluşturulması ve yönetimi Kayıt Defteri Anahtarlarını ve Değerlerini değiştirme ve görüntüleme Modyfing Kontrol Paneli Ayarları Kullanıcıları ve Grupları Yönetme Etki Alanı Yapısını Yönetme Active Directory Nesneleri Oluşturma ve Silme Linux'ta Süreçleri Yönetme Dosya & Klasörleri Manipüle Etme Boru ile Çalışma Sistem İzleme Komutları

• Süreç Yönetimi & İş Kontrolü • Servis Yönetimi							Linux Hizmetlerini Yönetme
Veritabanı sistemi yönetimi • Depolar & Kaynak Listeleri • Web Sunucusunu Yönetme • Sistem Günlükleri & Günlük İzleme • Linux'ta Görevleri Zamanlama • Sunucu & Ağ Sorunları • Yedekleme & Kurtarma • GRUB'un Güvenliğini Sağlama • Güvenlik duvarları • Active Directory Nesneleri & GPO Yönetimi • DNS & DHCP • PowerShell Temelleri • Microsoft BitLocker, AppLocker & Güvenlik Duvarı • LDAP & Kerberos • NTLM Hakkında • Şifre & Kilitleme Politikaları • Kimlik Doğrulama & Erişim Kontrolü • İnternet Kontrol Mesajı Protokolü (ICMP) • TCP ve UDP karşılaştırması • NetBIOS & SMB • SSL & TLS • Sertifika • Telnet ve Secure Shell (SSH) Protokolleri • HTTP & HTTPS • Posta Sistemleri Protokolleri • Etki Alanı Adı Sistemi Protokolü (DNS) • FTP & RDP • Kapsülleme Vs. Dekapsülasyon • Ağ Sniffers & Wireshark • TCP/UDP • DHCP, DNS	4	0,5	2	0,5	**7**	**3,5**	Depoları ve Kaynak Listelerini Yönetme Web Sunucusunu Yönetme Sistem Günlüklerini ve Günlük İzlemeyi doğrulama ve yönetme Linux'ta Görevleri Zamanlama Sunucu Sorun Giderme Yedekleri Geri Yükleme GRUB'un Güvenliğini Sağlama Veritabanı hizmetlerini yönetme Parola İlkelerini Ayarlama Hesap Kilitleme İlkelerini Ayarlama Kimlik Doğrulama ve Erişim Kontrolünü Ayarlama
Ağ yönetimi • Ağ Türleri & Kablosuz Ağlar • Ağlar & Topolojiler • Cihazlar Kimlik & Erişim Cihazları • Altyapı & Güvenlik Cihazları • Özel Cihazlar & Ağ Mimarisi • Sanal Ağlar • Fiziksel ve Mantıksal Adresler • OSI & Ağ Modelleri • Veri Kapsülleme ve Kapsül Çıkarma • Ağ Protokolleri ve Bağlantı Noktası Numaraları	4	0,5	2	0,5	**7**	**3,5**	Ağ Topolojileri Oluşturma Ağ Cihazlarını Yönetme Ağı Oluşturmak Ağ Cihazlarının Güvenliğini Sağlama Sanal Ağlar Oluşturma Ağ Protokollerini ve Bağlantı Noktası Numaralarını Ayarlama Cisco Packet Tracer ile çalışma

• Ağ Ortamı ve Kabloları • Kablosuz Teknolojiler • Ağ Yönetim Araçları • Cisco Paket İzleyici • Ağ Sınıfları & Alt Ağ Oluşturma • Adres Çözümleme Protokolü (ARP) • Statik ve Dinamik IP Adresleme • Ağ Adresi Çevirisi (NAT) • Anahtarlar & Cisco IOS • Switch Port Güvenlik & Router Arayüzleri • VLAN'ları ve DTP'yi yapılandırma • VLAN'lar Arası Yönlendirme • ACL'lere Giriş • Ağ Sorun Giderme							Adres Çözümleme Protokolü (ARP) ile çalışma Ağ Planlama Statik ve Dinamik IP Adreslemeyi Ayarlama DHCP ve NAT'ı Yapılandırma Cisco IOS ile çalışma VLAN'ları yapılandırma Ağ Sorun Giderme
Bulut yönetimi • Hipervizörler & Sanal Makineler • Konteyner • Sanal Ortamların Güvenliğini Sağlama • Yedekleme & Kurtarma • Bulut Bilişim & CSP'ler • Bulut Hizmet Modelleri Nelerdir? • Bulut Dağıtım Türleri • Sanal Ağlar • AWS İşlem Hizmetleri • Amazon Esnek İşlem Bulutu (EC2) • Bulut İzleme Araçları • Otomasyon ve Orkestrasyon Araçları • Bulut Güvenliği Tehditleri ve Güvenlik Açıkları • Kimlik ve Erişim Yönetimi (IAM) • Rol Tabanlı Erişim Kontrolü (RBAC) • Çok Faktörlü Kimlik Doğrulama (MFA) • Bulut Veri Şifreleme • Sanal Özel Bulut (VPC) • Docker & Kubernetes	4	0,5	2	0,5	**7**	**3,5**	Sanal Makineler Oluşturma Konteynerleri Ayarlama Sanal Ortamların Güvenliğini Sağlama Yedeklemelerle Çalışma Bulut Ağ Yönetimi Sanal Ağları Yapılandırma Bulut İzleme Araçlarıyla Çalışmak Otomasyon ve Orkestrasyonun Uygulanması Bulut Güvenliği Tehditlerini ve Güvenlik Açıklarını Tespit Etme Kimlik ve Erişim Yönetimi'ni (IAM) ayarlama Bulut Veri Şifrelemesini Uygulama Docker ve Kubernetes ile çalışma
Siber-fiziksel sistem yönetimi • Güvenlik & Erişim Kontrolleri • Kimlik Doğrulama Türleri • TACACS+ ve RADIUS • AAA Yapılandırması • Risk Yönetimi Hedefleri • Şifreleme & Şifre Çözme • Hashing & Rainbow Tabloları • MAC Sahtekarlığı & ARP Zehirlenmesi • VLAN Atlama & Rogue DHCP • ICMP Sel • TCP & UDP Sel	4	0,5	2	0,5	**7**	**3,5**	Altyapı Ana Bileşenlerinin Kurulması Güvenlik Kontrollerinin Uygulanması TACACS+ ve RADIUS ile çalışma AAA Yapılandırması Şifreleme ve Şifre Çözme ile Oynamak Yaygın saldırıları ve savunma tekniklerini analiz etme

• Oturum Ele Geçirme • DNS Sahtekarlığı • Derinlemesine Savunma (DID) & Sıfır Güven • Askerden Arındırılmış Bölgeler (DMZ'ler) • Bal Küpleri & Ağ Güçlendirme • Güvenli Bir Ağ için En İyi Uygulamalar • VPN'ler • SSH & VNC • Durum Bilgisi Olan ve Durum Bilgisi Olmayan Güvenlik Duvarları • Ana Bilgisayar Tabanlı ve Ağ Tabanlı • Donanım ve Yazılım Güvenlik Duvarları • Web Uygulaması Güvenlik Duvarı (WAF) • Güvenlik Duvarlarında Yapay Zeka • IDS & IPS • NIDS & HIDS • Snort • tcpdump							Askerden Arındırılmış Bölgelerin (DMZ'ler) Kurulması Bal Küplerini Araştırmak Güvenli Bir Ağ için En İyi Yöntemlerle Sağlamlaştırma VPN yükleme Secure Shell (SSH) ile çalışma Sanal Ağ Bilgi İşlem (VNC) ile çalışma Güvenlik Duvarı Çalışma Teknikleri Yapay Zekanın Güvenlik Duvarlarına Uygulanması Koruma ve algılama için Snort ve tcpdump kullanma
Sistem güçlendirme • GenAI Teknikleri • Kod Oluşturma • Kullanıcı Hesabı Yönetimi ve Erişim Kontrolü • Anomali Tespiti ve Sorun Giderme • Apache2 Hizmet Hatalarını Çözme • Yama Yönetimi & Güncellemeler • Otomatik Yedekleme & Kurtarma • BT Varlık Yönetimi ve Envanter • GenAI ile Silinen Dosyaları Kurtarma • Siber Güvenlik Prosedürleri • Tehdit Tespiti & Analizi • Tehdit Yanıtı ve İyileştirme • Gerçek Zamanlı Tehdit Tespiti için Yapay Zekadan Yararlanma • GenAI Modellerinin Doğrulanması ve Test Edilmesi • Yönetişim ve Düzenleyici Çerçeveler • DNS Yapılandırma & Güvenlik • DHCP Yapılandırma & Güvenlik • PowerShell Temelleri • Anahtar Bağlantı Noktası Güvenliği • Ağ Temel Giriş/Çıkış Sistemi (NetBIOS)	4	0,5	2	0,5	**7**	**3,5**	GenAI Teknikleriyle Çalışmak Kullanıcı Hesabı Yönetimi ve Erişim Kontrolü Anomali Tespiti ve Sorun Giderme GenAI ile Apache2 Hizmet Hatalarını Çözme Yama Yönetimini ve Güncellemeleri Yapılandırma Otomatik Yedekleme ve Kurtarma'yı ayarlama BT Varlıklarını Yönetme GenAI ile Silinen Dosyaları Kurtarma DNS ve DHCP Güvenliğini Uygulama Microsoft BitLocker ve Microsoft AppLocker ile çalışma Microsoft Güvenlik Duvarı'nı kurma Anahtar Bağlantı Noktası Güvenliğini Ayarlama Dosya Aktarım Protokolünün (FTP) Güvenliğini Sağlama

• Sunucu İleti Bloğu Protokolü (SMB) • Güvenli Yuva Katmanı (SSL) & Taşıma Katmanı Güvenliği (TLS) • Güvenlik Sertifikaları • Posta Sistemleri Protokolleri • Etki Alanı Adı Sistemi Protokolü (DNS) • Dosya Aktarım Protokolü (FTP) • Uzak Masaüstü Protokolü (RDP) • Linux'ta Görevleri Zamanlama • Sunucu Sorun Giderme • Ağ Sorun Giderme • Yedekleme & Kurtarma • GRUB'un Güvenliğini Sağlama • Güvenlik Duvarlarını Kurma & Güvence Altına Alma							Uzak Masaüstü Protokolü (RDP) Güvenliğini Sağlama Linux'ta Güvenlik Görevlerini Zamanlama GRUB'un Güvenliğini Sağlama Güvenlik Duvarlarını Kurma & Güvence Altına Alma (iptables)
Kullanılabilirlik • IR ve SOC • Olaylar ve Olaylar • Uyarı Tespiti & Uyarı Triyajı • Dokümantasyon ve Raporlama • Web Saldırıları Nedir? • DoS ve DDoS • SQL Enjeksiyonu & XSS • Komut Enjeksiyonu & Yerel Dosya Dahil Etme (LFI) • Siteler Arası İstek Sahteciliği (CSRF) • Brute-Force & Credential Stuffing • Hash'i Geç & Bileti Geç • LDAP Keşif • Bozuk Erişim Kontrolü • Fidye yazılımı • Bilgisayar Virüsü & Solucanı • Truva Atı & Reklam Yazılımı • Keylogger & Cryptojacking • Dosyasız Kötü Amaçlı Yazılım • Kötü Amaçlı Yazılımın Yayılmasını Anlamak • Statik ve Dinamik Zararlı Yazılım Analizi • Güvenli Kötü Amaçlı Yazılım Ana-lizi • Hibrit Analiz Kötü Amaçlı Yazılım Araştırması • Statik ve Dinamik Kötü Amaçlı Yazılım Analizi Gerçekleştirme • IOC'leri ve Şifre Politikalarını Yönetme • Kabul Edilebilir Kullanım İlkeleri (AUP)	4	0,5	3	0,5	**8**	4	Olayları ve Olayları Tespit Etme Uyarı Triyajı Gerçekleştirme Dokümantasyon ve Doğru Raporlama Yapılması Olay Sonrası Faaliyetlerin Uygulanması DoS ve DDoS'a karşı şekillendirme ve koruma Web saldırılarını ve Kötü Amaçlı Yazılımların Yayılmasını Tespit Etme Güvenli Statik ve Dinamik Kötü Amaçlı Yazılım Analizi Gerçekleştirme IOC'leri yönetmek Parola İlkelerini Ayarlama Kendi Cihazını Getir (KCG) İlkelerini Ayarlama Uzaktan Erişim İlkelerini Ayarlama

• Kendi Cihazını Getir (KCG) Politikaları • Uzaktan Erişim İlkeleri							
Toplam	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Değerlendirme stratejisi	**Karşılaştırmalı ağırlık yüzdesi**	**Değerlendirme kriterleri**
Öz değerlendirme testi (1)	5%	10 puan - %95-100 doğru cevap. 9 puan – %85-94 doğru cevap. 8 puan – %75-84 doğru cevap. 7 puan - %65-74 doğru cevap. 6 puan – %55-64 doğru cevap. 5 puan – %45-54 doğru cevap. 4 puan – %35-44 doğru cevap. 3 puan – %25-34 doğru cevap. 2 puan – %15-24 doğru cevap. 1 puan – %0-14 doğru cevap.
Öz değerlendirme testi (2)	5%	
Öz değerlendirme testi (3)	5%	
Öz değerlendirme testi (4)	5%	
Öz değerlendirme testi (5)	5%	
Öz değerlendirme testi (6)	5%	
Öz değerlendirme testi (7)	5%	
Bilgi değerlendirme testi	65%	

3. M3: ANALITIK ARAÇLAR

Modül başlığı	**Modül kodu**
ANALİTİK ARAÇLAR	

Öğretim Üyesi(ler)	**Modülün teslim edildiği kurum veya departman**

Dersin veriliş şekli	**Dil**
Yüz yüze, çevrimiçi, hibrit	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
Hiç kimse

Tahsis edilen AKTS kredisi sayısı	**Öğrencinin iş yükü**	**İletişim çalışma saatleri**	**Bireysel çalışma saatleri**
3	75	50	25

Modülün amacı ve sonuçları		
Bu kursu bitirdikten sonra öğrenciler, performans ölçümlerini, veri analitiğini ve güvenlik istihbaratını kullanarak kurumsal varlıkları koruma becerileriyle donatılacaktır. Potansiyel siber güvenlik risklerini ve güvenlik açıklarını belirlemek için analitik araçları etkili bir şekilde uygulamayı, güvenlik önlemlerini geliştirmek için veriye dayalı içgörülerden yararlanmayı ve parolalar, tarayıcı kullanımı, e-posta ve veri işleme uygulamalarıyla ilgili performans ölçümlerini kullanmayı öğrenecekler. Modülün sonunda katılımcılar, uygun araçları kullanarak potansiyel güvenlik tehditlerini değerlendirip azaltabilecek ve herhangi bir tehdit veya kesintiyi doğru düzenleyici kanallara bildirebileceklerdir.		
Modülün öğrenme çıktıları	**Öğretim ve öğrenme yöntemleri**	**Değerlendirme yöntemleri**
Bilgi: Öğrenciler, kurumsal varlıkları korumak için performans ölçümlerinin, veri analitiğinin ve güvenlik istihbaratının nasıl uygulanacağı konusunda pratik bilgiler edineceklerdir.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. [Öğretim Yöntemleri, örneğin teorik dersler, konuk konuşmacılar, sınavlar, oyunlar, pratik görevler/laboratuvarlar, akranlar arası öğretme ve öğrenme, kendi kendine öğrenme vb.] D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı"	Öz değerlendirme testleri Bilgi değerlendirme testi
Beceriler: Öğrenciler, potansiyel siber güvenlik risklerini ve güvenlik açıklarını belirlemek için analitik araçları kullanma, siber güvenlik uygulamalarını güçlendirmek için veriye dayalı içgörüler uygulama ve parolaların, taramanın, e-postanın ve veri işlemenin güvenliğini değerlendirmek ve geliştirmek için performans ölçümlerini kullanma becerisine sahip olacaklardır.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. [Öğretim Yöntemleri, örneğin pratik görevler/laboratuvarlar, uygulamalı etkinlikler, simüle edilmiş ortamlar, sınavlar, oyunlar, vaka çalışmaları vb.] D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı"	Pratik değerlendirmeler
Yeterlilikler: Öğrenciler, analitik araçları kullanarak potansiyel güvenlik tehditlerini değerlendirme ve azaltma, tehditleri ve ihlalleri kuruluşlarındaki uygun kanallara doğru bir şekilde bildirme konusunda yetkin olacaklardır.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. [Öğretim Yöntemleri, örn. simüle edilmiş ortamlar, bayrak yarışmalarını ele geçirme, 5E'ler, CBL, CL, POGIL, PBL vb.] D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı"	Simülasyon Yarışma

Modül içeriği: konuların dökümü	İletişim çalışma saatleri	Bireysel çalışma saatleri ve görevler

	Dersler (HEI)	Danışma	Uygulama (HEI)	Test	**Tüm iletişim çalışmaları**	**Bireysel çalışma**	**Görev**
Performans ölçümleri (metrikler) • Performans Metrikleri • Sistem ve Ağ İzleme • Performans Metriklerini İzleme • Ağ Haritalama • Güvenlik Açığı Taraması • Ağ Trafiği Analizi	10	0,5	5	0,5	**16**	**8,5**	• Performans ölçümleri ve araçları hakkında araştırma yapın. Performans izleme araçlarını karşılaştırın ve farklılıklarını belirleyin. • Zabbix kurulumunu tamamlayın ve temel yapılandırmayı gerçekleştirin. • Zabbix ile performans ölçümlerini izlemek için bir uygulama oluşturun. • Ağ haritalama yazılımı (nmap, rustscan vb.) kullanarak hedef sistemdeki güvenlik açıklarını belirleyin • Nessus yazılımını kullanarak hedef sistemde bir zafiyet taraması gerçekleştirin. Bir güvenlik açığı test raporu hazırlayın. • Wireshark kullanarak ağ trafiği analizi gerçekleştirin.
Veri analitiği • Veri koleksiyonu • Veri Temizleme ve Ön İşleme • Veri Analizi • Veri Görselleştirme • Analitik Araçlar • Siber Güvenlikte Veri Analitiği Uygulamaları	10	0,5	5	0,5	**16**	**8,5**	• Varsayımsal bir KOBİ için hazırlanmış siber güvenlik sorunlarıyla ilgili bir veri kümesi üzerinde veri temizleme ve ön işleme adımlarını gerçekleştirin. • Varsayımsal KOBİ'den temizlenmiş ve önceden işlenmiş veri kümesini analiz edin ve sonuçları görselleştirin. • Siber güvenlikte veri analizi uygulamalarına örnekler nelerdir? Lütfen araştırın.
Güvenlik istihbaratı • Güvenlik İstihbaratını Anlamak • Güvenlik İstihbaratının Kaynakları	10	0,5	7	0,5	**18**	**8**	• Güvenlik istihbaratının KOBİ'lerin proaktif güvenlik stratejilerine

• Tehdit İstihbaratı Toplama Yöntemleri • Tehdit İstihbaratı Çerçeveleri • Yapay Zeka Odaklı Güvenlik İstihbarat Platformları • Güvenlik İstihbaratı Uygulamalarına İlişkin Örnek Olay İncelemeleri							nasıl katkıda bulunduğunu araştırın. • Güvenlik istihbaratı elde etmek için en yaygın kaynaklar nelerdir? Bu kaynakların güvenilirliğini nasıl değerlendiriyorsunuz? • Her tehdit istihbaratı toplama yönteminin avantajlarını ve sınırlamalarını tanımlayın. • MITRE ATT&CK ve Cyber Kill Chain gibi tehdit istihbaratı çerçevelerinin temel özelliklerini açıklayın. • Güvenlik istihbaratının kullanıldığı gerçek bir vaka çalışmasını inceleyin. Bu vaka çalışmasında kullanılan istihbarat toplama yöntemlerini açıklayın.
Toplam	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Değerlendirme stratejisi	Karşılaştırmalı ağırlık yüzdesi	Değerlendirme kriterleri
Öz değerlendirme testi I	15%	10 puan - %95-100 doğru cevap. 9 puan – %85-94 doğru cevap. 8 puan – %75-84 doğru cevap. 7 puan - %65-74 doğru cevap. 6 puan – %55-64 doğru cevap. 5 puan – %45-54 doğru cevap. 4 puan – %35-44 doğru cevap. 3 puan – %25-34 doğru cevap. 2 puan – %15-24 doğru cevap. 1 puan – %0-14 doğru cevap.
Öz değerlendirme testi II	15%	
Öz değerlendirme testi III	15%	
Bilgi değerlendirme testi	55%	

Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*
Gerekli okuma
...
Önerilen kaynaklar
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4: GÜVENLIK OPERASYONLARI

Modül başlığı	Modül kodu
GÜVENLİK İŞLEMLERİ	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman

Dersin veriliş şekli	Dil
Yüz yüze, çevrimiçi, karma, istişareler	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
Hiç kimse

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	75	50	25

Modülün amacı ve sonuçları

Bu dersi bitirdikten sonra öğrenciler, BİT altyapıları, sistemleri ve hizmetleri içindeki güvenlik operasyonlarını etkin bir şekilde yönetebileceklerdir. Güvenlik operasyonlarıyla ilgili en iyi uygulamaları, araçları ve çerçeveleri uygulayarak siber güvenlik olaylarını izleme, tespit etme, bunlara yanıt verme ve bunlardan kurtulma becerilerini kazanacaklar.

Modülün öğrenme çıktıları	Öğretim ve öğrenme yöntemleri	Değerlendirme yöntemleri
Bilgi: Öğrenciler, izleme, tespit, olay müdahalesi ve kurtarma dahil olmak üzere güvenlik operasyonları hakkında ileri düzeyde bilgi edineceklerdir. Siber güvenlik standartlarına uygun olarak KOBİ işyerlerinin özel ihtiyaçlarına göre uyarlanmış etkili siber güvenlik operasyonel rutinleri oluşturabilecek ve tanımlayabileceklerdir.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. [Öğretim Yöntemleri, örneğin teorik dersler, literatür analizi, konuk konuşmacılar, akranlar arası öğretme ve öğrenme, mentorluk vb.] D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı"	Öz değerlendirme testleri Bilgi değerlendirme testi

Beceriler: Öğrenciler, güvenlik operasyonları görevlerini yerine getirmek, etkili izleme stratejileri tasarlamak ve uygulamak, olaylara müdahale etmek ve KOBİ işyerleri için özel olarak tasarlanmış sağlam operasyonel rutinler geliştirmek için gelişmiş metodolojileri ve araçları uygulama becerisine sahip olacaklardır.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. *[Öğretim Yöntemleri, örneğin teorik dersler, literatür analizi, konuk konuşmacılar, akranlar arası öğretme ve öğrenme, mentorluk vb.]* D2.3 "*KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı*"	Öz değerlendirme testleri Bilgi değerlendirme testi
Yeterlilikler: Öğrenciler, KOBİ işyerleri için stratejik güvenlik operasyonları politikaları ve prosedürleri geliştirme ve uygulama konusunda yetkin olacaklardır.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. *[Öğretim Yöntemleri, örneğin teorik dersler, literatür analizi, konuk konuşmacılar, akranlar arası öğretme ve öğrenme, mentorluk vb.]* D2.3 "*KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı*"	Öz değerlendirme testleri Bilgi değerlendirme testi

Modül içeriği: konuların dökümü	**İletişim çalışma saatleri**					**Bireysel çalışma saatleri ve görevler**	
	Dersler (HEI)	Danışmalar	Uygulama (HEI)	Test	Tüm iletişim	Bireysel çalışma	Görev
Güvenlik Operasyonlarının temelleri - Güvenlik Operasyonlarını ve SOC'yi (Güvenlik Operasyonları Merkezi) Anlamak - Güvenlik Operasyonlarındaki roller ve sorumluluklar - Güvenlik operasyonları araçlarına ve teknolojilerine genel bakış	6	0,5	2	0,5	**9**	6	Bir SOC'nin yapısını ve işlevini tanımlayın ve anlayın, güvenlik operasyonlarındaki çeşitli rolleri, güvenlik operasyonlarında kullanılan araştırma araçlarını analiz edin ve bir vaka çalışmasını analiz edin.

Güvenlik Yakınsaması - Güvenlik yakınsamasını anlama - Fiziksel güvenliğin temelleri (fiziksel güvenlik ilkeleri, fiziksel varlıkların korunması, politikalar) - Güvenlik yakınsaması ilkelerini vurgulayan örnek olay incelemesi	8	0,5	4	0,5	**13**	6	Güvenlik yakınsamasının tanımını ve ilkelerini gözden geçirin, fiziksel ve dijital güvenlik operasyonlarını entegre etmenin önemini kabul edin, Siber ve fiziksel alanlardaki riskleri tanımlayın ve değerlendirin.
Güvenlik Bilgileri ve Olay Yönetimi - Güvenlik izleme ilkelerinin gözden geçirilmesi - SIEM çözümlerinin uygulanması	8	0,5	4	0,5	**13**	6	Güvenlik izleme ve SIEM uygulamasına giriş. Günlük türleri, algılama yöntemleri ve izleme yaşam döngüsü gibi temel ilkeler. Mimari, veri toplama, kural oluşturma ve uyarı yönetimi dahil olmak üzere SIEM dağıtmanın pratik yönleri.
Güvenlik Operasyonları Uygulamaları - Veri kaynaklarını belirleyin ve günlük toplamayı optimize edin - SIEM ile uyarıları merkezileştirme - SIEM'inizi test etme	4	0,5	10	0,5	**15**	7	Çeşitli BT ortamlarında günlük yönetimi, SIEM yapılandırması ve tehdit algılama konularında temel bilgi ve pratik becerilere sahip kapsamlı ve uygulamaya yönelik eğitim programı.
Toplam	**26**	**2**	**20**	**2**	**50**	**25**	

Değerlendirme stratejisi	**Karşılaştırmalı ağırlık yüzdesi**	**Değerlendirme kriterleri**

Öz değerlendirme testi (1)	10%	10 puan - %95-100 doğru cevap. 9 puan – %85-94 doğru cevap. 8 puan – %75-84 doğru cevap. 7 puan - %65-74 doğru cevap. 6 puan – %55-64 doğru cevap. 5 puan – %45-54 doğru cevap. 4 puan – %35-44 doğru cevap. 3 puan – %25-34 doğru cevap. 2 puan – %15-24 doğru cevap. 1 puan – %0-14 doğru cevap.
Öz değerlendirme testi (2)	10%	
Öz değerlendirme testi (3)	10%	
Öz değerlendirme testi (4)	10%	
Bilgi değerlendirme testi	60%	

Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*

Gerekli okuma

Cybellium (2024). *Güvenlik Operasyon Merkezleri (SOC) Çalışma Kılavuzu: Güvenlik Operasyon Merkezlerini (SOC) Öğrenmek İçin Kapsamlı Bir Kılavuz*

Muniz, J. (2021). *Modern Güvenlik Operasyonları Merkezi*. Pearson Eğitimi.

ENISA (2017). *Olay Müdahalesi ve Siber Kriz İşbirliği Stratejileri*. **Olaylara müdahale ve siber kriz işbirliği stratejileri — ENISA (europa.eu)**

Önerilen kaynaklar

Basta, A., Basta, N., Anwar, W., Essar, MI (2024). Açık Kaynak Güvenlik Operasyonları Merkezi (SOC): Modern bir SOC oluşturmaya, yönetmeye ve sürdürmeye yönelik eksiksiz bir kılavuz.

Sibelit (2023). Güvenlik operasyonları merkezini (SOC) yönetme.

5. M5: GÜVENLIK YÖNETIŞIMI VE POLITIKASI

Modül başlığı	Modül kodu
GÜVENLİK YÖNETİMİ & POLİTİKASI	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman

Dersin veriliş şekli	Dil
Yüz yüze / Online / Hibrit	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
Hiç kimse

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	75	50	25

Modülün amacı ve sonuçları
"Güvenlik Yönetişimi ve Politikası" konusu, öğrencileri KOBİ'lerde siber güvenliğin zorluklarıyla yüzleşmeye hazırlamayı, güvenlik yönetişimini iş stratejisine entegre etmeyi ve GDPR gibi yasal düzenlemelere uyumu sağlamayı amaçlamaktadır. Modül, tehditlerin ve güvenlik açıklarının belirlenmesi, sağlam ve uyarlanabilir güvenlik politikalarının tasarlanması ve olayların etkili bir şekilde yönetilmesi gibi hususları kapsar. Ayrıca, kuruluşta net roller atayan ve siber güvenliği stratejik hedeflerle uyumlu hale getiren yönetişim yapıları geliştirmeye odaklanır. Öğrenciler, siber risk değerlendirmesi ve azaltma konusunda teknik yeterlilikler kazanacak ve güvenlik olgunluğunda iyileştirmeler önermek için analiz becerileri geliştireceklerdir. Ayrıca siber güvenlik ihtiyaçlarını yöneticilere etkili bir şekilde iletme, bilinçli karar almayı destekleme ve siber güvenlikte mevzuata uygunluk ve etik sağlama konusunda da beceri kazanacaklar. "Güvenlik Yönetimi & Politikası" modülü ayrıca phishing önleme, AI destekli siber saldırılar ve fidye yazılımı yönetimi üzerine odaklanmış bir incelemeyi içerir, bu belirli tehditlerin yönetişim ve uyum için entegre bir yaklaşım gerektirdiğini analiz eder. Güvenlik politikalarının etkinliği yalnızca olayları önleme yetenekleriyle değil, aynı zamanda ortaya çıkan tehditlere uyum sağlama ve mevcut yasal düzenlemelere uyum sağlama yetenekleriyle de ölçülecektir.

Modülün öğrenme çıktıları	Öğretim ve öğrenme yöntemleri	Değerlendirme yöntemleri

Bilgi: Öğrenciler, mevcut siber güvenlik ilkelerini, trendlerini ve sektörleriyle ilgili ulusal ve uluslararası mevzuata uyumu dahil ederek, KOBİ işyerlerinde yeni siber güvenlik rutinlerinin ve iş akışlarının nasıl uygulanacağı konusunda ileri düzeyde bilgi edineceklerdir. Kimlik avı önlemeyi entegre etme, yapay zeka odaklı tehditleri yönetme ve KOBİ ortamlarında fidye yazılımlarına yanıt verme konusunda ileri düzeyde bilgi edinin	**Dersler (Yönlendirilmiş Okumalar):** Dersler siber güvenlik, yönetişim, gizlilik ve uyumluluk konularında sağlam bir kavramsal temel sağlayacak ve aktif öğrenci katılımını teşvik edecektir. Düzenli Q&A oturumları, anketler ve canlı problem çözme egzersizlerini içeren etkileşimli dersler içerir. Mentimetre ve Poll Everywhere gibi araçları kullanarak, **Tartışmalara ve Forumlara Katılım:** Tartışmalara ve forumlara katılım, öğrencilerin siber güvenlik konularını tartışmalarına ve eleştirel bir şekilde analiz etmelerine olanak tanıyarak tartışma becerilerini geliştirecektir. Siber güvenlikte etik, politikalar ve karar verme ile ilgili konulara uygulanacaktır. **Vaka Çalışmaları:** Vaka çalışmaları, öğrencilerin KOBİ'lerdeki siber güvenlik durumlarını analiz etmelerine ve gerçek sorunları çözmek için teorik bilgileri uygulamalarına olanak tanıyacaktır. Veri ihlali yönetimi, fidye yazılımı, kimlik avı, Yapay Zeka Odaklı Saldırılar, güvenlik politikası uygulaması ve yönetişim gibi konulara odaklanacaklar.	**Öz değerlendirme testleri:** Kendi kendine testler, öğrencilerin çeşitli sorular aracılığıyla her bir alt konuya ilişkin anlayışlarını değerlendirmelerine olanak tanır ve iyileştirme alanlarını belirlemek için sürekli geri bildirim sağlar. Final notunu etkilemezler, ancak kendi kendine öğrenmenin anahtarıdırlar. **Final Sınavı (İsteğe Bağlı):** Final sınavı isteğe bağlıdır ve öğrencilerin gelişimsel sorular, vaka analizi ve çoktan seçmeli olarak derse ilişkin genel anlayışlarını değerlendirerek bitirme sertifikası almalarına olanak tanır. Geçmenin bitirme sertifikası alması gerekirken, almayanlara katılım sertifikası verilecektir.
Beceriler: Öğrenciler, risk değerlendirmeleri yapmak, yeni siber güvenlik rutinleri tasarlamak ve uygulamak ve müdahale stratejileri hazırlamak için gelişmiş metodolojileri kullanma becerisine sahip olacak, KOBİ işyerlerinde etkili yönetişim ve uyumluluk sağlayacaktır. Gelişmiş tehditleri ele alan ve kurumsal uyumluluğu sağlayan kapsamlı siber güvenlik rutinleri	**Uygulamalı Atölye Çalışmaları:** Uygulamalı atölye çalışmaları, öğrencilerin eğitmenden gerçek zamanlı geri bildirim alarak politika geliştirme ve olay simülasyonları gibi alıştırmalar yoluyla siber güvenlik kavramlarını uygulamalarına olanak tanıyacaktır. Pratik becerileri güçlendirmek ve öğrencileri öğrendiklerini gerçek durumlarda uygulamaya hazırlamak için tasarlanmıştır. **Pratik Çalışma ve Bireysel Projeler:**	**Pratik Değerlendirmeler:** Kurs boyunca yapılan pratik değerlendirmeler, öğrencilerin KOBİ'ler bağlamında gerçek sorunları çözme yeteneklerini değerlendirmek amacıyla teorik bilgileri siber güvenlik politikası geliştirme ve olay simülasyonları gibi simüle edilmiş durumlara uygulamalarına olanak

tasarlama ve uygulama becerilerini geliştirin.	Pratik çalışmalar ve bireysel projeler, öğrencilerin politika yazma ve risk analizi, özerk çalışma becerilerini geliştirme ve teorik bilgilerin pratik uygulaması gibi görevler aracılığıyla siber güvenlik kavramlarını uygulamalarına olanak tanıyacaktır. **İşbirlikçi Projeler:** İşbirlikçi projeler, öğrencilerin güvenlik politikaları ve yönetişim modelleri de dahil olmak üzere KOBİ'ler için siber güvenlik çözümleri geliştirmek üzere ekipler halinde çalışmasına olanak tanıyacaktır. Öğretmenlerden ve akranlardan gelen geri bildirimlerle ekip çalışmasını, proje yönetimini ve edinilen bilgilerin pratik uygulamasını teşvik edeceklerdir.	tanıyacaktır. **Grup Projeleri:** Grup projeleri, öğrencilerin risk tanımlamadan yönetişim modelleri ve olay müdahale planlarının önerilmesine kadar hem içeriğin kalitesini hem de işbirliği yapma yeteneğini değerlendiren kapsamlı bir siber güvenlik projesi geliştirmelerine olanak tanıyacaktır. Bu proje, nihai değerlendirmenin anahtarıdır ve tüm ders öğrenimini bütünleştirir.
Yeterlilikler: Öğrenciler, stratejik siber güvenlik politikaları geliştirme ve uygulama, KOBİ işyerlerinde yeni rutinler ve iş akışları oluşturmaya yönelik girişimlere liderlik etme ve kurumsal hedefler ve uyumluluk gereklilikleriyle uyumlu etik kararlar alma konusunda yetkin olacaklardır. Karmaşık siber tehditleri önleyen ve uluslararası siber güvenlik düzenlemelerine uyumu sağlayan siber güvenlik politikalarını formüle etme ve yürütme konusunda yetkin olun.	**Senaryo Simülasyonları:** Senaryo simülasyonları, öğrencilerin siber güvenlik olaylarını gerçek saldırıları taklit eden sanal ortamlarda yönetmelerine ve baskı altında stratejik kararlar almalarına olanak tanıyacaktır. Bu yöntem, kriz yönetimi ve olaylara müdahale becerilerini geliştirir ve kritik durumlarda güvenlik politikası değerlendirmesi ve karar vermeyi öğretmenin anahtarıdır. Öğrencilerin, kimlik avı saldırıları, Fidye Yazılımı ve Yapay Zeka Odaklı Saldırılar gibi belirli olayları önlemek veya bunlara yanıt vermek için yönetişim politikalarını nasıl uygulayacaklarını göstermeleri gerekecektir; ilgili düzenleyici çerçeveye ilişkin anlayışlarını değerlendirmek.	**Simülasyonlar ve Olay Yönetimi:** Öğrenciler, bir KOBİ'deki gerçek krizleri taklit eden simülasyonlarda siber güvenlik olaylarını yönetme becerilerine göre değerlendirilecektir. Amaç, baskıyla başa çıkma, stratejik kararlar alma ve müdahale planlarını gerçek zamanlı olarak yürütme yeteneklerini ölçmek ve bunların dinamik durumlardaki pratik uygulamalarını değerlendirmektir.

Modül içeriği: konuların dökümü	İletişim çalışma saatleri					Bireysel çalışma saatleri ve görevler	
	Dersler (HEI)	Danışmalar	Uygulama (HEI)	Test	Tüm iletişim	Bireysel	Görev
Organizasyonel bağlam -KOBİ'lerde siber güvenliğin evrimi-Mevcut büyük tehditler ve güvenlik açıkları-Siber güvenliğin iş stratejisi üzerindeki etkisi-KOBİ'lerde büyük işletmelere karşı siber güvenliğin belirli zorlukları - Siber güvenlik uygulamalarının düzenleyici etkilerini ve bunların yönetişim yapılarıyla nasıl uyumlu olduğunu anlayın. - Sınırlı bütçeler, özel güvenlik personelinin eksikliği ve siber güvenlik yatırımlarına öncelik vermek için pratik yöntemler gibi KOBİ'lere özgü yaygın siber güvenlik zorlukları.	5	0,5	3	0,5	**9**	**4**	Okuma, araştırma, örnek olay incelemesi hazırlama
Gizlilik -Siber güvenlikte gizlilik ilkeleri-Kişisel verilerin korunması ve GDPR-Gizliliğin KOBİ operasyonlarına etkisi-Gizliliğin korunmasına yönelik araçlar ve teknikler	4	0,5	3	0,5	**8**	**4**	Politika analizi, bireysel atama
Yasalar, etik ve uyumluluk -Siber Güvenlik Kuruluşları, Politikaları ve Standartları -İlgili ulusal ve uluslararası mevzuat -KOBİ'lerde mevzuata uygunluk -Siber Güvenlikte Etik -Siber güvenlikte uyumsuzluğun hukuki sonuçları - Siber güvenlik yönetişimini güçlendirmek ve sürekli izleme ve otomatik tehdit yanıtı yoluyla uyumluluğu sağlamak için yapay zeka tabanlı araçların nasıl kullanılabileceğinin analizi.	5	0,5	3	0,5	**9**	**5**	Örnek olay, mevzuat analizi

Güvenlik idaresi -Siber güvenlik yönetişim yapısı-Güvenlik yönetiminde rol ve sorumluluklar-Siber güvenlik olgunluk modelleri-Siber güvenliğin kurumsal yönetime entegrasyonu - Simüle edilmiş kriz koşulları altında risk değerlendirmeleri yapma ve stratejik müdahale planları oluşturma becerilerini geliştirin (Fidye yazılımı, kimlik avı saldırısı, ...)	4	0,5	3	0,5	**8**	**4**	Risk yönetimi senaryo analizi
Yönetici ve yönetim kurulu düzeyinde iletişim -Siber güvenlik iletişim stratejileri-Üst yönetime güvenlik raporlaması-Güvenlik verilerine dayalı karar verme-Siber güvenlikte kriz yönetimi ve iletişim - Yapay zeka odaklı saldırılar ve fidye yazılımlarını içeren yüksek stresli senaryolarda kriz yönetimi ve karar verme becerilerinde uzmanlaşın.	4	0,5	3	0,5	**8**	**4**	Sunum hazırlama, paydaş iletişimi
Yönetim politikası -Güvenlik politikası geliştirme-Politika uygulama ve izleme-Politikaların değerlendirilmesi ve sürekli iyileştirilmesi-Güvenlik politikalarının teknolojik ve mevzuat değişikliklerine uyarlanması - Etkili eğitim ve farkındalık politikalarının mevzuata uygunluk ve risk azaltmanın ne kadar önemli bir bileşeni olabileceğinin araştırılması.	4	0,5	3	0,5	**8**	**4**	Bir politika belgesinin yazılması ve revizyonu
Toplam	**26**	**3**	**18**	**3**	**50**	**25**	

Değerlendirme stratejisi	**Karşılaştırmalı ağırlık yüzdesi**	**Değerlendirme kriterleri**
Kendi kendine test I	10%	Örgütsel bağlamda temel kavramların değerlendirilmesi.
Kendi kendine test II	10%	Özel hayatın gizliliği ile ilgili temel kavramların değerlendirilmesi.
Kendi kendine test III	10%	Yasaların, etik ve uyum politikalarının değerlendirilmesi.
Kendi kendine test IV	10%	Siber güvenlik politikalarının değerlendirilmesi.
Kendi kendine test V	10%	Yönetici düzeyinde iletişimin değerlendirilmesi.
Kendi kendine test VI	10%	Güvenlikte yönetsel politikaların değerlendirilmesi ve politika oluşturulması.
Bilgi değerlendirme testi	40%	Tüm ders konularına ilişkin bütünleştirici soruları kapsayan final sınavı.

10 puan - %95-100 doğru cevap.
9 puan – %85-94 doğru cevap.
8 puan – %75-84 doğru cevap.
7 puan - %65-74 doğru cevap.
6 puan – %55-64 doğru cevap.
5 puan – %45-54 doğru cevap.
4 puan – %35-44 doğru cevap.
3 puan – %25-34 doğru cevap.
2 puan – %15-24 doğru cevap.
1 puan – %0-14 doğru cevap.

Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*

Gerekli okuma

...

"AB Siber Güvenlik Yasası: Dijital Çağda Dayanıklılık ve Tutarlılığın Yönetilmesi" , Luisa Marin

- Bu kitap, siber güvenlik yönetişiminin AB bağlamında nasıl yapılandırıldığını ve uygulandığını anlamak için çok önemli olan AB'nin siber güvenlik yasalarının ve politikalarının derinlemesine bir analizini sunmaktadır.

"Avrupa Birliği'nde Siber Güvenlik: Yönetişim Politikasında Dayanıklılık ve Uyarlanabilirlik", George Christou

- Bu kitap, AB içindeki siber güvenlik için yönetişim çerçevelerini ve politika oluşturma süreçlerini araştırıyor ve öğrencilerin farklı yönetişim seviyeleri arasındaki dinamik etkileşimi anlamalarına yardımcı oluyor.

"Kimlik Avı ve Karşı Önlemler: Artan Elektronik Kimlik Hırsızlığı Sorununu Anlamak" , Markus Jakobsson ve Steven Myers

- AB'ye özgü olmasa da, bu kitabın kimlik avı teknikleri ve karşı önlemlerin ayrıntılı araştırması, GDPR uyumluluğuna ve veri koruma ilkelerine odaklanarak AB içinde bağlamsallaştırılabilir.

"Avrupa Siber Güvenlik Yasası ve Yönetmeliği", Nadya Purtova ve Bert-Jaap Koops tarafından düzenlendi

- Bu düzenlenmiş cilt, uyumluluk zorlukları ve NIS Direktifi ve GDPR gibi çerçeveler de dahil olmak üzere Avrupa Birliği'ndeki siber güvenliğe özgü yasal ve düzenleyici önlemleri kapsar.

"Fidye Yazılımı: Dijital Şantajı ve Kuruluşunuza Yönelik Tehdidini Anlamak" , Allan Liska ve Timothy Gallo

- AB'ye özgü vaka çalışmaları ve örneklerle desteklenen bu metin, öğrencilerin AB düzenlemeleri kapsamında fidye yazılımı saldırılarının sonuçlarını anlamalarına yardımcı olacaktır.

Önerilen kaynaklar

"AB Genel Veri Koruma Yönetmeliği (GDPR): Bir Yorum", Lukas Feiler ve Nikolaus Forgó

- Bu yorum, AB'deki düzenleyici ortamı ve bunun siber güvenlik uygulamaları üzerindeki etkisini anlamak için gerekli olan GDPR'ye ilişkin ayrıntılı bilgiler sunmaktadır.

"Avrupa'da Veri Koruma ve Siber Güvenlik: Yasal Çerçeveler ve Pratik Hususlar", Paul Lambert

- Bu kitap, düzenlemelere uyum ve güvenlik önlemleri için en iyi uygulamalar da dahil olmak üzere AB'deki veri koruma ve siber güvenlik stratejilerinin uyumlaştırılmasına ilişkin pratik bilgiler sunmaktadır.

"Ağ ve Bilgi Güvenliği: Avrupa ve Uluslararası Perspektifler", Jeanne Pia Mifsud Bonnici ve Joe Cannataci tarafından düzenlendi

- Bu koleksiyon, ağ ve bilgi güvenliği ortamını hem Avrupa hem de uluslararası perspektiflerden inceleyerek AB'nin siber güvenlik çabaları için daha geniş bir bağlam sağlıyor.

"Siber Güvenlikte Yapay Zeka: Uygulamalar, Zorluklar ve Etik", Elena Fersman ve Martin Fredriksson

- Yapay zeka teknolojilerinin siber güvenliğe entegrasyonuna ilişkin kapsamlı bir genel bakış, özellikle AB bağlamında geçerli olan etik, operasyonel ve düzenleyici zorlukları ele alıyor.

"Dijital Çağda Siber Güvenlik: Araçlar, Teknikler ve Uygulamalar", Gregory B. White, Eric A. Fisher ve James L. Antonakos

- Yalnızca AB'ye odaklanmasa da, bu kitap çok çeşitli modern siber güvenliği de kapsamaktadır

Çalışma *materyali (HackerU ve Cybint orijinal materyalleri)*
Gerekli okuma
• TCP/IP Ağ Yönetimi: Unix Sistem Yöneticileri için Yardım 3. Baskı, Craig Hunt (O'Reilly) • Temel Sistem Yönetimi Cep Referansı: Komutlar ve Dosya Biçimleri (Cep Yöneticisi), Eleen Frisch (O'Reilly) • Bilgisayar Ağı: Bilgisayar Ağları, İnternet ve OSI Modelinde Uzmanlaşmak için Başlangıç Kılavuzu, Ramon Nastase
Önerilen kaynaklar
• CompTIA A+ Sertifikası Tüm Bir Arada Dummies (Bilgisayar/Teknoloji) 5. Baskı Glen E. Clarke, Edward Tetz, Timothy L. Warner tarafından • Nikhil Abraham tarafından Aptallar İçin Kodlama All-in-One 1. Baskı • Bilgi Teknolojisi Temelleri Cilt 1: Eric Frick tarafından Bilgi Sistemlerine Giriş • Aptallar İçin BT Mimarisi 1. Baskı Kalani Kirk Hausman, Susan L. Cook tarafından • Cybersecurity For Dummies (Bilgisayar/Teknoloji) 1. Baskı Steinberg tarafından • Linux For Dummies, 10. Baskı 10. Baskı Richard Blum tarafından • Windows 10 For Dummies, 3. Baskı (Bilgisayar/Teknoloji) 3. Baskı Rathbone tarafından • Doug Lowe tarafından yazılan Aptallar İçin Ağ 12.

6. M6: SIBER GÜVENLIK PLANLAMASI

Modül başlığı	Modül kodu
SİBER GÜVENLİK PLANLAMASI	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman

Dersin veriliş şekli	Dil
Yüz yüze, çevrimiçi, karma, istişareler	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
-

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	75	50	25

Modülün amacı ve sonuçları

Bu dersi bitirdikten sonra öğrenciler siber güvenlik planlaması ve yönetiminin temel ilkelerini anlayabilecek ve uygulayabileceklerdir. Uluslararası standartları ve çerçeveleri uygulama, uzun vadeli güvenlik stratejileri geliştirme, operasyonel ve taktiksel siber güvenlik önlemlerini yönetme ve bulut ve sıfır güven gibi güvenli ağ mimarilerini planlama becerisi kazanacaklar. Ayrıca öğrenciler, gelişen tehditler karşısında kurumsal dayanıklılık ve etkili siber güvenlik önlemleri sağlayarak etkili olay müdahale planları tasarlayacak ve iş sürekliliği stratejilerini uygulayacak donanıma sahip olacaklardır.

Modülün öğrenme çıktıları	Öğretim ve öğrenme yöntemleri	Değerlendirme yöntemleri
Bilgi: Öğrenciler, gelişmiş siber güvenlik ilkelerinin ve güncel trendlerin stratejik planlama ve operasyonel yönetime nasıl entegre edileceği konusunda ileri düzeyde bilgi edineceklerdir	Anlatım, Örnek Olaylar, Grup Tartışmaları, Kendi Kendine Öğrenme	Öz değerlendirme testleri, Bilgi değerlendirme testleri
Beceriler: Öğrenciler, ortaya çıkan riskleri ele alan ve sağlam taktiksel yanıtlar sağlayan siber güvenlik stratejilerini etkili bir şekilde tasarlamalarına ve uygulamalarına olanak tanıyan stratejik planlama ve operasyonel yönetim konusunda beceri kazanacaklardır	Pratik alıştırmalar, Atölye çalışmaları, Vaka çalışmaları	Proje bazlı değerlendirmeler, Pratik değerlendirmeler
Yeterlilikler: Öğrenciler, stratejik siber güvenlik çerçeveleri geliştirme ve uygulama, siber güvenlik girişimlerini yönetme ve yönetme konusunda yetkin olacaklardır	Atölye Çalışmaları, Seminerler, Rol Yapma Egzersizleri	Sürekli değerlendirme, Senaryo tabanlı test

Modül içeriği: konuların dökümü	İletişim çalışma saatleri					Bireysel çalışma saatleri ve görevler	
	Dersler (HEI)	Danışma	Uygulama (HEI)	Test	**Tüm iletişim çalışmaları**	**Bireysel çalışma**	**Görev**
1. Siber Güvenlik Planlamasına Giriş: Veri, insan ve toplum güvenliği - Veri Güvenliği - Bilgi Depolama Güvenliği, Soruşturma süreci - Veri güvenliği - Parola saldırı teknikleri -İnsan Güvenliği -Farkındalık ve Anlayış - Toplumsal güvenlik – Siber Suçlar nedir, Siber etik - Toplumsal güvenlik - Siber hukuk- Dijital deliller, Dijital sözleşmeler, Çok uluslu sözleşmeler (anlaşmalar)	8	0,5	6	0,5	**15**	**8**	KOBİ'lerde verilerin yasal yönlerini, insan ve toplum güvenliğini, verileri yöneten yasaları ve politikaları tanımlayın. KOBİ'lerle ilgili siber saldırı türlerini sınıflandırın Siber saldırıları önlemek için yararlı araçları belirleyin
2. Stratejik Planlama -Siber Güvenlik Amaç ve Hedeflerinin Tanımlanması -SWOT Analizi (Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler) -Uzun vadeli güvenlik stratejileri geliştirmek -Temel Performans Göstergelerinin (KPI'lar) Belirlenmesi -Güvenlik Stratejisinin Gözden Geçirilmesi ve Güncellenmesi	8	2	6	2	**18**	**8**	Bir SWOT analizi kullanarak KOBİ'lerle ilgili siber güvenlik hedeflerini tanımlayın, riskleri ele almak için uzun vadeli stratejiler geliştirin, kaynakları ve bütçeyi buna göre tahsis edin, ilerlemeyi ölçmek için KPI'lar belirleyin ve stratejiyi yeni tehditlere göre düzenli olarak güncelleyin.
3. Operasyonel ve Taktik Yönetim -Erişim Kontrollerinin Uygulanması -Yama Yönetimi ve Yazılım Güncel-lemeleri -Sürekli Sistem İzleme - Çalışan Güvenliği Farkındalık Eğitimi	8	1	6	2	**17**	**9**	Yetkisiz erişimi kısıtlamak için erişim kontrolü önlemleri uygulayın, yama yönetimi yoluyla sistemleri koruyun, olağandışı faaliyetler için izleme kurun ve çalışanlara siber güvenlik farkındalığı eğitimi sağlayın.
Toplam	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Değerlendirme stratejisi	Karşılaştırmalı ağırlık yüzdesi	Değerlendirme kriterleri
Öz değerlendirme testi (1)	10%	10 puan - %96-100 doğru cevap. 9 puan – %91-95 doğru cevap. 8 puan – %86-90 doğru cevap. 7 puan - %80-85 doğru cevap. 6 puan – %70-79 doğru cevap. 5 puan – %60-69 doğru cevap. 4 puan – %50-59 doğru cevap. 3 puan – %40-49 doğru cevap. 2 puan – %30-39 doğru cevap. 1 puan – %0-29 doğru cevap.
Öz değerlendirme testi (2)	10%	
Öz değerlendirme testi (3)	10%	
Bilgi değerlendirme testi	70%	

Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*

Gerekli okuma

1. Nair, A., & Greeshma, M. R. (2023). Bilgi Güvenliği Uyumluluk Yönetiminde Uzmanlaşmak: ISO/IEC 27001:2022 Uyumluluğu Üzerine Kapsamlı Bir El Kitabı. Packt Yayıncılık Limited.
2. Falco, G. J., & Rosenbach, E. (2021). Siber Riskle Yüzleşmek: Siber Güvenlik için Gömülü Bir Dayanıklılık Stratejisi. Oxford Üniversitesi Yayınları.
3. NIST Siber Güvenlik Çerçevesi (CSF) 2.0, Ulusal Standartlar ve Teknoloji Enstitüsü, 26 Şubat 2024

Önerilen kaynaklar

1. Mehta, S. (2023). *ISACA Sertifikalı Risk ve Bilgi Sistemleri Kontrolü (CRISC®) Sınav Kılavuzu*. Packt Yayıncılık Limited.
2. Gregory, PH (2021). *CISM Sertifikalı Bilgi Güvenliği Yöneticisi Hepsi Bir Arada Sınav Kılavuzu*. McGraw-Tepesi.
3. ISACA. (2021). *CRISC İnceleme Kılavuzu, 7. baskı*. ISACA.
4. Avrupa Parlamentosu ve Konseyi. (2022, 14 Aralık). *Finans sektörü için dijital operasyonel dayanıklılığa ilişkin (AB) 2022/2554 sayılı Yönetmelik*.
5. Genel Veri Koruma Yönetmeliği (GDPR) Kılavuzu, Bilgi Komiserliği Ofisi

7. M7: RISK YÖNETIMI VE AZALTMA

Modül başlığı	Modül kodu
RISK YÖNETIMI VE AZALTMA	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman

Dersin veriliş şekli	Dil
Yüz yüze, çevrimiçi, karma, istişareler	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
Hiç kimse

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	75	50	25

Modülün amacı ve sonuçları		
Bu dersi bitirdikten sonra öğrenciler, risk analizi, değerlendirme ve tedaviyi planlayarak, uygulayarak, raporlayarak ve ileterek BİT altyapılarının, sistemlerinin ve hizmetlerinin siber güvenlikle ilgili risklerini sürekli olarak yönetebileceklerdir (tanımlama, analiz etme, değerlendirme, tahmin etme, azaltma).		
Modülün öğrenme çıktıları	**Öğretim ve öğrenme yöntemleri**	**Değerlendirme yöntemleri**
Bilgi: Öğrenciler, risk tanımlama, değerlendirme ve kontrol dahil olmak üzere risk yönetimi süreçleri hakkında ileri düzeyde bilgi edinecek ve ulusal ve uluslararası standartlara uygun olarak KOBİ işyerlerinin özel ihtiyaçlarına göre uyarlanmış etkili siber güvenlik rutinleri oluşturmalarına ve tanımlamalarına olanak tanıyacaktır	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. *[Öğretim Yöntemleri, örneğin teorik dersler, literatür analizi, konuk konuşmacılar, akranlar arası öğretme ve öğrenme, mentorluk vb.]* D2.3 "*KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı*"	Öz değerlendirme testleri Bilgi değerlendirme testi
Beceriler: Öğrenciler, kapsamlı risk değerlendirmeleri yapmak, etkili risk yönetimi stratejileri tasarlamak ve uygulamak ve KOBİ işyerleri için özel olarak tasarlanmış sağlam siber güvenlik rutinleri geliştirmek için gelişmiş metodolojileri ve araçları uygulama becerisine sahip olacaklardır	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. *[Öğretim Yöntemleri, örneğin pratik görevler/laboratuvarlar, sınavlar, oyunlar, teknik video analizi, vaka çalışmaları, uygulamalı etkinlikler vb.]* D2.3 "*KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı*"	Öz değerlendirme testleri Bilgi değerlendirme testi
Yeterlilikler: Öğrenciler, KOBİ işyerleri için stratejik siber güvenlik politikaları geliştirme ve uygulama konusunda yetkin olacaklardır	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. *[Öğretim Yöntemleri, örneğin yarışmalar, CTF, simüle edilmiş ortamlar, 5E'ler, CBL, CL, PBL vb.]* D2.3 "*KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı*"	Öz değerlendirme testleri Bilgi değerlendirme testi

Modül içeriği: konuların dökümü	İletişim çalışma saatleri					Bireysel çalışma saatleri ve görevler	
	Dersler (HEI)	Danışma	Uygulama (HEI)	Test	Tüm iletişim çalışmaları	Bireysel çalışma	Görev
Risk değerlendirmesi Genel risk yönetimi süreci Genel risk yönetimi çerçevesi Risk yönetimi ilkeleri Risk yönetimi standartları Pratik örnekler	2	0	2	0	**4**	5	Risk tanımlama, değerlendirme ve kontrol dahil olmak üzere risk yönetimi sürecindeki temel adımları kısaca özetleyin. Bir KOBİ için risk yönetiminin iç ve dış bağlamlarını tanımlayın. Risk değerlendirmesinin kapsamını belirtin ve temel risk faktörlerini belirleyin. Seçilen KOBİ'ye özel risk kriterleri geliştirin.
Risk tanımlama Risk yönetiminde liderlik ve bağlılık Risk yönetimi faaliyetlerinin kapsamının tanımlanması Risk yönetimi bağlamının dış ve iç bağlamı Maddi ve Maddi Olmayan Risk Kaynakları Nedenler ve olaylar Tehditler ve fırsatlar Güvenlik açıkları ve yetenekler Dış ve iç bağlamdaki değişiklikler Ortaya çıkan risklerin göstergeleri Varlıkların ve kaynakların doğası ve değeri Sonuçlar ve hedefler üzerindeki etkileri Bilginin sınırlılıkları ve bilginin güvenilirliği İlgili kişilerin önyargıları, varsayımları ve inançları	4	0	4	0	**8**	5	KOBİ için hem maddi hem de manevi risk kaynaklarını belirleyin. Riskleri nedenlere, olaylara, tehditlere ve fırsatlara göre kategorilere ayırın. KOBİ'nin iç güvenlik açıklarını ve yeteneklerini analiz edin ve hem dış hem de iç bağlamlardaki değişikliklerin işletmeyi nasıl etkileyebileceğini değerlendirin. KOBİ için ortaya çıkan potansiyel riskleri belirleyin ve bunları izlemek için göstergeler önerin. Varlıkların ve kaynakların doğasının ve değerinin bu analizi nasıl etkilediğini düşünün

Pratik örnekler ve vaka çalışmaları							
İçeriden gelen tehditler İçeriden gelen tehditlerin tanımı ve türleri İçeriden gelen tehditlerin maliyetleri İçeriden tehdit azaltma programı oluşturma İçeriden gelen tehditleri tespit etme ve tanımlama İçeriden gelen tehditlerin değerlendirilmesi İçeriden gelen tehditleri yönetme Pratik örnekler ve vaka çalışmaları	6	0	6	0	**12**	5	KOBİ'lerle ilgili farklı türde içeriden gelen tehditleri tanımlayın ve sınıflandırın. Bu tehditlerin işletmeye getirebileceği potansiyel maliyetleri tartışın. Bir KOBİ için temel bir içeriden tehdit azaltma programı geliştirin. Tespit, tanımlama ve yönetim stratejileri gibi temel bileşenleri vurgulayın. İçeriden gelen tehditleri değerlendirmek için bir yöntem önerin ve bu tehditleri KOBİ bağlamında etkili bir şekilde yönetmek için atılacak adımları ana hatlarıyla belirtin
Risk ölçme ve değerlendirme modelleri ve metodolojileri Nicel ve nitel risk değerlendirme modelleri ve metodolojileri Olayların olasılığı ve sonuçları Sonuçların niteliği ve büyüklüğü Karmaşıklık ve bağlantı; Zamanla ilgili faktörler ve oynaklık Mevcut kontrollerin etkinliğinin değerlendirilmesi Hassasiyet ve güven seviyeleri Pratik örnekler ve vaka çalışmaları	6	0	6	0	**12**	5	Bir nicel ve bir nitel risk değerlendirme modelini karşılaştırın ve karşılaştırın. Bir risk olayının olasılığını ve bir KOBİ için sonuçlarının niteliğini ve büyüklüğünü değerlendirin. Karmaşıklığın, zamanla ilgili faktörlerin ve oynaklığın bu değerlendirmeyi nasıl etkilediğini düşünün. Belirlenen risklerin yönetilmesinde mevcut kontrollerin etkinliğini değerlendirin. Kontrol önlemlerine duyarlılık ve güven düzeylerinin bir analizini dahil edin
Risk kontrolü Risk tedavisi seçeneklerinin	6	0	6	0	**12**	5	KOBİ'ler için uygun risk tedavisi seçeneklerini

formüle edilmesi ve seçilmesi Risk tedavisinin planlanması ve uygulanması Bu tedavinin etkinliğinin değerlendirilmesi Kalan riskin kabul edilebilir olup olmadığına karar vermek İzleme ve inceleme Kayıt ve Raporlama Pratik örnekler ve vaka çalışmaları							belirleyin ve seçin. Seçiminizi ilgili risklerin niteliğine göre gerekçelendirin. Seçilen tedavi seçeneklerinin bir KOBİ ortamında nasıl uygulanacağını özetleyen kısa bir risk tedavi planı geliştirin. Risk tedavisinin etkinliğini değerlendirmek ve kalan riskin kabul edilebilir olup olmadığını belirlemek için bir yöntem önerin
Toplam	**24**	**2**	**24**	**0**	**50**	**25**	

Değerlendirme stratejisi	**Karşılaştırmalı ağırlık yüzdesi**	**Değerlendirme kriterleri**
Öz değerlendirme testi (1)	5%	10 puan - %95-100 doğru cevap. 9 puan – %85-94 doğru cevap. 8 puan – %75-84 doğru cevap. 7 puan - %65-74 doğru cevap. 6 puan – %55-64 doğru cevap. 5 puan – %45-54 doğru cevap. 4 puan – %35-44 doğru cevap. 3 puan – %25-34 doğru cevap. 2 puan – %15-24 doğru cevap. 1 puan – %0-14 doğru cevap.
Öz değerlendirme testi (2)	5%	
Öz değerlendirme testi (3)	5%	
Öz değerlendirme testi (4)	5%	
Öz değerlendirme testi (5)	5%	
Bilgi değerlendirme testi	75%	

	Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*
	Gerekli okuma
1.	Adarsh Nair ve Greeshma M. R. (2023) Bilgi Güvenliği Uyumluluk Yönetiminde Uzmanlaşmak: ISO/IEC 27001:2022 Uyumluluğu Üzerine Kapsamlı Bir El Kitabı. Packt Yayıncılık, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&query=risk%20management**
2.	Gregory J. Falco, Eric Rosenbach (2021) Siber Riskle Yüzleşmek: Siber Güvenlik için Gömülü Bir Dayanıklılık Stratejisi. Oxford üniversitesi yayınları, e-Kitap
3.	Kristina Narvaez, Betty Simkins, John Fraser (2014) Kurumsal Risk Yönetiminin Uygulanması: Vaka Çalışmaları ve En İyi Uygulamalar. John Wiley & Oğulları
-	ENISA (2022) Risk Yönetimi Standartları

4.	(AB) 2010/2014 sayılı Tüzüğü ve (AB) 2018/1972 sayılı Direktifi değiştiren ve (AB) 2016/1148 sayılı Direktifi (NIS 2 Direktifi) yürürlükten kaldıran, Birlik genelinde yüksek düzeyde ortak siber güvenlik önlemlerine ilişkin 14 Aralık 2022 tarih ve (AB) 2022/2555 sayılı Avrupa Parlamentosu ve Konsey Direktifi (AB) 2022/2555 sayılı Direktifi
5.	ISO 31000 Risk yönetimi — Yönergeler
	Önerilen kaynaklar
-	Shobhit Mehta (2023) ISACA Sertifikalı Risk ve Bilgi Sistemleri Kontrolü (CRISC®) Sınav Kılavuzu. Packt Yayıncılık, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management**
-	Peter H. Gregory (2021) CISM Sertifikalı Bilgi Güvenliği Yöneticisi Hepsi Bir Arada Sınav Kılavuzu. McGraw-Tepesi
-	ISACA (2021) CRISC İnceleme Kılavuzu 7. baskı. ISACA Hakkında
-	Avrupa Parlamentosu ve Konseyi'nin finans sektörü için dijital operasyonel esnekliğe ilişkin 14 Aralık 2022 tarihli ve (AB) 2022/2554 sayılı Tüzüğü ve (AB) 1060/2009, (AB) 648/2012, (AB) 600/2014, (AB) 909/2014 ve (AB) 2016/1011 sayılı Tüzükleri tadil eden Tüzük

8. M8: İŞ SÜREKLILIĞI, FELAKET KURTARMA VE OLAY YÖNETIMI & PERSONEL GÜVENLIĞI

Modül başlığı	Modül kodu
İŞ SÜREKLILIĞI, FELAKET KURTARMA VE OLAY YÖNETIMI & PERSONEL GÜVENLIĞI	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman

Dersin veriliş şekli	Dil
Yüz yüze, çevrimiçi, karma, istişareler	*İngilizce, Fince, Türkçe, Norveççe, Litvanca, Rumence, Fransızca, Lehçe, İspanyolca*

Önkoşullar
Hiç kimse

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	75	50	25

Modülün amacı ve sonuçları

Bu dersi tamamlayan öğrenciler, kapsamlı iş sürekliliği ve felaket kurtarma (BC/DR) planlarını formüle edebilecek ve yönetebilecek, işlevsel bir olay yönetimi programı geliştirebilecek ve güçlü ve etkili bir personel güvenliği politikası oluşturabilecektir. Öğrenciler, varlıkları nasıl koruyacaklarını, aşırı kayıp deneyimlerinden kaçınmayı nasıl sağlayacaklarını, arıza sürelerini nasıl önleyeceklerini, kriz durumlarından ve kriz yönetimi ortamlarından nasıl kaçınacaklarını veya sınırlayacaklarını öğreneceklerdir.

Bu kursu tamamlayan öğrenciler, tüm ulusal ve uluslararası yasalara uygun olarak entegre edilmiş gelişmiş siber güvenlik ilkeleri ve teknolojileri kullanarak KOBİ'ler için kapsamlı bir siber güvenlik el kitabının sürekli uygulanmasını yazabilecek ve izleyebileceklerdir. Öğrenciler ayrıca uygulamayı takip edecekler.

Modülün öğrenme çıktıları	Öğretim ve öğrenme yöntemleri	Değerlendirme yöntemleri
Bilgi: Öğrenciler, gelişmiş siber güvenlik ilkelerini, en son savunma mekanizmalarını ve olay yönetimi, iş sürekliliği ve personel güvenliğinde ulusal ve uluslararası mevzuat ve standartlara bağlılığı içeren kapsamlı bir KOBİ işyeri siber güvenlik el kitabının nasıl oluşturulacağı ve uygulanacağı konusunda ileri düzeyde bilgi edineceklerdir	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı" [Öğretim Yöntemleri]	Öz değerlendirme testleri, Bilgi değerlendirme testi

Beceriler: Öğrenciler, riskleri değerlendirmek, etkili risk yönetimi ve olay müdahale stratejileri tasarlamak ve kuruluşlarının ihtiyaçlarına göre uyarlanmış kapsamlı iş sürekliliği planları geliştirmek için gelişmiş metodolojiler kullanarak bir KOBİ işyeri siber güvenlik el kitabı oluşturma ve sürdürme becerisine sahip olacaklardır.	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı" [Öğretim Yöntemleri]	Öz değerlendirme testleri, Bilgi değerlendirme testi
Yeterlilikler: Öğrenciler, KOBİ'ler için bir siber güvenlik el kitabı geliştirme ve uygulama, güvenlik projelerini ve ekiplerini etkili bir şekilde yönetme, kurumsal hedefler ve uyumluluk yükümlülükleriyle uyumu sağlama konusunda yetkin olacaklardır	Öğretim üyesi tarafından Bölüm 1.3'ten seçilecektir. D2.3 "KOBİ Siber Güvenlik Değişim Aracıları Öğrenme Yolunun Yapısı" [Öğretim Yöntemleri]	Öz değerlendirme testleri, Bilgi değerlendirme testi

Modül içeriği: konuların dökümü	**İletişim çalışma saatleri**					**Bireysel çalışma saatleri ve görevler**	
	Dersler (HEI)	Danışma	Uygulama (HEI)	Test	**Tüm iletişim**	**Bireysel**	**Görev**
Olay yanıtı - Siber güvenlikte olay müdahalesinin tanımı ve önemi - Etkili bir olay müdahalesi kurtarmanın temel bileşenleri - Yaygın siber güvenlik tehditlerine genel bakış (kimlik avı, içeriden gelen tehditler,) - Olay Müdahale Planının (IRP) Geliştirilmesi - Olay Müdahale Ekibindeki roller ve sorumluluklar - Olayı Simüle Etmek: sahte bir plan yürütmek.	5	0,5	3	0,5	**9**	**5**	Bir siber güvenlik olayı sırasında roller, sorumluluklar ve atılacak adımlar dahil olmak üzere KOBİ'niz için ayrıntılı bir Olay Müdahale Planı geliştirin. Planınızın etkinliğini test etmek için bir olayı simüle edin ve sahte bir tatbikat yapın.
Olağanüstü durum kurtarma - Felaket Kurtarmayı Anlamak - Felaket Kurtarma Planı Geliştirme - Felaket Kurtarma'daki roller ve sorumluluklar - Felaketten sonra kurtarma adımları	5	0,5	3	0,5	**9**	**5**	Yıkıcı bir olaydan sonra BT altyapısını ve verilerini geri yükleme prosedürlerini özetleyen bir Felaket Kurtarma Planı oluşturun. İyileşme için bir zaman çizelgesi ekleyin ve sürecin her aşaması için ekip üyelerine sorumluluklar atayın.

İş sürekliliği - İş sürekliliğini anlamak - İş Sürekliliği Planının (BCP) Geliştirilmesi - İş sürekliliğinde rol ve sorumluluklar - İş Etki Analizi - BCP'yi test etme ve iyileştirme	5	0,5	3	0,5	**9**	**5**	Bir kesinti sırasında ve sonrasında kritik iş fonksiyonlarının çalışır durumda kalmasını sağlayan bir İş Sürekliliği Planı tasarlayın. Temel hizmetleri ve kaynakları belirleyin ve bunları çeşitli senaryolar altında sürdürmek için acil durum stratejilerinin ana hatlarını çizin.
Güvenlik bilinci, eğitim ve öğretim - Güvenlik farkındalığını anlamak - Güvenlik eğitim programı geliştirme - Siber güvenlikte çalışan sorumlulukları - Güvenlik farkındalığının etkinliğini ölçme -	1	0,5	2	0,5	**4**	**1**	KOBİ'niz için temel siber güvenlik politikalarına ve en iyi uygulamalara odaklanan bir güvenlik farkındalığı eğitim programı geliştirin. Çalışanlar için bir eğitim oturumu düzenleyin ve sınavlar veya etkileşimli etkinlikler aracılığıyla anlayışlarını değerlendirin.
Güvenlik işe alma uygulamaları - Güvenlik rolleri gereksinimlerini tanımlama - Geçmiş kontrolleri boyunca yürütmek - Güvenlik bileşenleri için görüşme - Devam eden değerlendirme ve geliştirme	1	0,5	2	0,5	**4**	**1**	Adayların siber güvenlik farkındalığını değerlendirmek için tasarlanmış geçmiş kontrolleri ve mülakat soruları dahil olmak üzere güvenlik odaklı işe alım uygulamaları oluşturun. Potansiyel çalışanlar için temel güvenlik nitelikleri ve özelliklerinden oluşan bir kontrol listesi oluşturun.

Güvenlik sonlandırma uygulamaları - Erişimi hemen iptal etme - Veri ve cihaz alma - Güvenlik içgörüleri için çıkış görüşmesi - İlgili ekiplerin bilgilendirilmesi - Yasal ve uyumluluk hususları	1	0,5	2	0,5	**4**	**2**	Erişimin iptal edilmesi, şirket varlıklarının kurtarılması ve çıkış görüşmelerinin yürütülmesine yönelik adımları içeren güvenli bir fesih prosedürü taslağı hazırlayın. Prosedürünüzün etkinliğini değerlendirmek için sahte bir sonlandırma senaryosu uygulayın.
Üçüncü taraf güvenliği - Üçüncü taraf riskinin değer-lendirilmesi - Tedarikçi seçiminde durum tespiti - Karşıtlıkların ve güvenlik ger-eksinimlerinin uygulanması - Sürekli izleme ve denetim - Olay müdahalesi ve iletişim	2	0,5	2	0,5	**5**	**2**	Üçüncü taraf satıcılarla ilişkili potansiyel riskleri belirleyin ve KOBİ'nizin siber güvenlik standartlarına uygunluklarını değerlendirmek için bir güvenlik değerlendirme kontrol listesi oluşturun. Güvenlik gereksinimlerini ve uyumsuzluk cezalarını içeren bir sözleşme şablonu taslağı hazırlayın.
İnceleme süreçlerinde güvenlik - Gözden geçirmelere güvenlik ekleme - Düzenli güvenlik denetimleri yapmak - Güvenlik açığı değerlendirmesi ve sızma testi - Olay sonrası incelemeler	1	0,5	1,5	0,5	**3, 5**	**2**	KOBİ'nizin siber güvenlik politikalarını ve prosedürlerini düzenli olarak gözden geçirmek ve güncellemek için bir süreç geliştirin. Tüm güvenlik önlemlerinin güncel ve ilgili standartlarla uyumlu olduğundan emin olmak için bir deneme denetimi planlayın ve gerçekleştirin.

Çalışanların kişisel bilgilerinin gizliliğine ilişkin özel sayı - Veri toplama sınırlamaları - Depolama ve erişim kontrolü - Gizlilik düzenlemelerine uygunluk - Veri paylaşımı ve üçüncü taraflar - Çalışan onayı ve hakları	2	0,5	2	0,5	**5**	**2**	Çalışanların kişisel bilgilerinin işlenmesi, veri koruma yasalarına ve en iyi uygulamalara uygunluğun sağlanmasına yönelik bir gizlilik politikası taslağı hazırlayın. Çalışan verilerinin nasıl saklandığı ve işlendiği konusundaki potansiyel güvenlik açıklarını belirlemek için bir risk değerlendirmesi yapın.
Toplam	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Değerlendirme stratejisi	**Karşılaştırmalı ağırlık yüzdesi**	**Değerlendirme kriterleri**
Öz değerlendirme testi (1)	5%	10 puan - %95-100 doğru cevap. 9 puan – %85-94 doğru cevap. 8 puan – %75-84 doğru cevap. 7 puan - %65-74 doğru cevap. 6 puan – %55-64 doğru cevap. 5 puan – %45-54 doğru cevap. 4 puan – %35-44 doğru cevap. 3 puan – %25-34 doğru cevap. 2 puan – %15-24 doğru cevap. 1 puan – %0-14 doğru cevap.
Öz değerlendirme testi (2)	5%	
Öz değerlendirme testi (3)	5%	
Öz değerlendirme testi (4)	5%	
Öz değerlendirme testi (5)	5%	
Bilgi değerlendirme testi	75%	

Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*

Gerekli okuma

- Gregory J. Falco, Eric Rosenbach (2021). *Siber Riskle Yüzleşmek: Siber Güvenlik için Gömülü Bir Dayanıklılık Stratejisi*. Oxford Üniversitesi Yayınları, e-Kitap.
- Michael Wallace, Lawrence Webber (2017). *Felaket Kurtarma El Kitabı: İş Sürekliliğini Sağlamak ve Hayati Operasyonları, Tesisleri ve Varlıkları Korumak için Adım Adım Plan*. AMACOM.
- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST). *Bilgi Teknolojisi Sistemleri için Acil Durum Planlama Kılavuzu*. NIST SP 800-34 Rev. 1.
- Cochran, K.A. (2024). Olay Müdahalesi, İş Sürekliliği ve Felaket Kurtarma. İçinde: Siber Güvenlik Temelleri. Apress, Berkeley, Kaliforniya. **https://doi.org/10.1007/979-8-8688-0432-8_14**

Önerilen kaynaklar

- ISACA (2023). *CISM İnceleme Kılavuzu 15*. ISACA.

- Peter H. Gregory (2021). *CISM Sertifikalı Bilgi Güvenliği Yöneticisi Hepsi Bir Arada Sınav Kılavuzu*. McGraw-Tepesi.
- BT Yönetişimi (2022). *ISO 22301:2019 – İş Sürekliliği Yönetim Sistemleri. Gereksinimler*.
- M. Souppaya, L. Feldman, G. Witte [2024], Siber Güvenlik Olaylarını Kurtarma Kılavuzu, Bilgisayar Güvenliği Bölümü Bilgi Teknolojileri Laboratuvarı Ulusal Standartlar ve Teknoloji Enstitüsü ABD Ticaret Bakanlığı
- Ihab Hanna Sawalha [2021]. İş sürekliliği ve felaket kurtarma ile ilgili görüşler. Uluslararası Acil Servisler Dergisi

EKLERİ

MÜFREDAT ŞABLONU

MODÜL AÇIKLAMASI

Modül başlığı	Modül kodu
...	

Öğretim Üyesi(ler)	Modülün teslim edildiği kurum veya departman
...	...

Dersin veriliş şekli	Dil
Yüz yüze, çevrimiçi, karma, istişareler	*İngilizce...*

Önkoşullar
...

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	İletişim çalışma saatleri	Bireysel çalışma saatleri
3	...	...	...

Modülün amacı ve sonuçları		
...		
Modülün öğrenme çıktıları	**Öğretim ve öğrenme yöntemleri**	**Değerlendirme yöntemleri**

Kaynakları kolaylaştırın (ekipman, yazılım, teknoloji)
...

Modül içeriği: konuların dökümü	İletişim çalışma saatleri					Bireysel çalışma saatleri ve görevler	
	Dersler (HEI)	Danışma	Uygulama (HEI)	Test	Tüm iletişim çalışmaları	Bireysel çalışma	Görev
1							
...							
n							
Toplam							

Değerlendirme stratejisi	Karşılaştırmalı ağırlık yüzdesi	Değerlendirme kriterleri
Kendi kendine test I		...
...		...
Kendi kendine test n		...
Bilgi değerlendirme testi		...

Çalışma materyali *(Soyadı, Adının Baş Harfi. (Yıl, Ay Gün). Makale başlığı. Dergi/Dergi/Gazete Başlığı, Cilt numarası (Sayı numarası), Makalenin tamamının sayfa numaraları, Yayınevi, URL)*
Gerekli okuma
...
Önerilen kaynaklar
...

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Temsilci-AB

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau