Co-funded by the European Union

# EQF SEVIYE 4-5

# MEÖ ÖĞRENCİLERİ İÇİN EĞİTİM MODÜLLERİ

CYBER AGENT 01.2025

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



www.cyberagents.eu

İş Paketi 3: Siber Güvenlik Değişim Aracıları Öğrenme Kaynağı Geliştirme

Çıktı 3.2: Mesleki Eğitim ve Öğretim öğrencileri için eğitim modülleri
3.2 Lideri – TIMTAL (TR)

# İÇERİK

TABLOLARIN LISTESI ..... 1
GIRIŞ ..... 2
1. CYBERAGENT EQF SEVIYE 4 PROGRAMININ AMAÇLARI ..... 3
2. AVRUPA YETERLILIKLER ÇERÇEVESI ..... 4
3. SIBER GÜVENLIK MESLEKI EĞITIM VE ÖĞRETIM ÖĞRENCILERI (EQF SEVIYE 4) ..... 5
3.1. EQF-4 için CYBERAGENT LEARNING Programı ..... 5
SON ..... 21

## TABLOLARIN LISTESI

Tablo 1-AYÇ Düzey-4 Öğrenme Çıktıları ..... 4
Tablo 2-Modül: 1 ..... 5
Tablo 3-Modül: 2 ..... 7
Tablo 4-Modül: 3 ..... 12
Tablo 5-Modül: 4 ..... 13
Tablo 6-Modül: 5 ..... 14
Tablo 7-Modül: 6 ..... 16
Tablo 8-Modül: 7 ..... 18
Tablo 9-Modül: 8 ..... 19

# GIRIŞ

Bilim ve teknolojideki hızlı değişimler, bireylerin ve toplumun değişen ihtiyaçları, öğrenme ve öğretme kuram ve yaklaşımlarındaki yenilikler ve gelişmeler bireylerden beklenen rolleri doğrudan etkilemiştir. Bu değişim, bilgiyi üreten, yaşamda işlevsel olarak kullanabilen, problem çözebilen, eleştirel düşünebilen, girişimci, kararlı, iletişim becerisine sahip, empati kurabilen, topluma ve kültüre katkıda bulunan vb. bireyi tanımlamaktadır.

Bilgi çağının getirdiği baş döndürücü hız, bireylerin ve toplumların sürekli değişen ihtiyaçlarını da beraberinde getirmektedir. Öğrenme ve öğretme kuramlarındaki yenilikler, bireylerden beklenen rolleri kökten değiştiriyor. Artık sadece bilgi sahibi olmak değil, o bilgiyi hayatta işlevsel olarak kullanabilmek, karmaşık sorunlara çözüm üretebilmek, eleştirel düşünebilmek, girişimci ruhla hareket edebilmek, etkili iletişim kurabilmek, empati kurabilmek ve topluma değer katabilmek gibi beceriler de ön plana çıkıyor. Bu dönüşüm, bireylerin sürekli öğrenmelerini, uyum sağlamalarını ve kendilerini geliştirmelerini teşvik eder.

Bu bağlamda, mesleki eğitim de büyük bir dönüşüm geçiriyor. Geleneksel meslekler yerini yeni, teknoloji odaklı ve sürekli gelişen mesleklere bırakıyor. Siber güvenlik, bu değişimde kritik bir öneme sahip. Çünkü dijitalleşen dünyada her sektörde ve her meslekte siber güvenlik riskleri artıyor. Siber güvenlik, kişisel verilerden kurumsal sırların korunmasına, kritik altyapıların güvenliğinden finansal işlemlerin güvenliğine kadar birçok alanda hayati bir rol oynar.

Mesleki eğitimde siber güvenlik eğitiminin önemi sadece teknik becerilerle sınırlı değildir. Etik değerlere sahip, sorumluluk duygusu yüksek, yasal düzenlemelere aşina ve sürekli öğrenmeye açık bireyler yetiştirmeyi de içerir. Çünkü siber güvenlik, sadece teknik bir sorun değil, aynı zamanda sosyal bir sorumluluktur. Bu nedenle, mesleki eğitimde siber güvenlik eğitimine gereken önemin verilmesi, hem bireylerin hem de toplumun geleceği için kritik bir adımdır.

Mesleki eğitim, eğitim sistemi bütünlüğü içinde tarım, sanayi ve hizmet sektörleri ile birlikte tüm mesleki ve teknik eğitim hizmetlerinin planlanması, araştırılması, geliştirilmesi, düzenlenmesi ve koordineli yönetimi, denetimi ve öğretimi faaliyetlerini kapsamaktadır. Bu eğitim faaliyetlerinin amacı, toplumun devamlılığını sağlayacak uzman bireyler ve üretimin her aşamasında ihtiyaç duyulan nitelikli elemanlar yetiştirmek, mesleki eğitime önem vermektir.

Siber Ajan mesleki eğitim programı (EQF4-5), bireyleri siber güvenlik yaşamına hazırlamak için tasarlanmıştır ve işgücü piyasası ihtiyaçlarına ve iş analizi yaklaşımına dayanmaktadır. Siber Ajan müfredatı, ilgili iş ve işlemleri gerçekleştirmek için sahip olunması gereken bilgi, beceri, tutum ve davranışları dersler ve kazanımlar yoluyla kazandırmayı amaçlarken, diğer yandan eğitim faaliyetleri de bu çerçeveye uygun olarak bireyleri iş hayatına hazırlayacak şekilde planlanmaktadır.

# 1. CYBERAGENT EQF SEVIYE 4-5 PROGRAMININ AMAÇLARI

Siber güvenlik ihtiyacı tüm dünyada olduğu gibi özellikle AB ülkelerinde de oldukça önemli hale geldi ve son yıllarda hızla arttı. Teknolojik gelişmelerle eş zamanlı olarak siber risk ve tehditler de aynı hızla değişmiş ve karmaşık bir hal almıştır. Siber risk ve tehditler, fiziksel saldırılardan çok daha kapsamlı ve olumsuz sonuçlara yol açacak bir potansiyele ulaşmıştır. Finans, elektronik haberleşme, enerji, ulaştırma ve havacılık gibi sektörlerin güvenli dijital ortamda hizmet vermesiyle, ulusal siber güvenliğin sağlanması ülkemiz için en önemli önceliklerden biri haline gelmiştir. Bu kapsamda örgün ve yaygın eğitimde siber güvenlik eğitiminin yaygınlaştırılması, eğitim içeriklerinin geliştirilmesi ve zenginleştirilmesi hedeflenmektedir.

## 2. AVRUPA YETERLILIKLER ÇERÇEVESI

AB, ulusal yeterliliklerin daha kolay anlaşılmasını ve daha karşılaştırılabilir olmasını sağlamak için bir çeviri aracı olarak Avrupa Yeterlilikler Çerçevesi'ni (AYÇ) geliştirmiştir. AYÇ, öğrencilerin ve çalışanların sınır ötesi hareketliliğini desteklemeyi, Avrupa çapında yaşam boyu öğrenmeyi ve mesleki gelişimi teşvik etmeyi amaçlamaktadır.

AYÇ, farklı ulusal yeterlilik çerçeveleri arasında bir çeviri aracı olarak hizmet veren, her tür yeterlilik için 8 seviyeli, öğrenme çıktılarına dayalı bir çerçevedir. Bu çerçeve, kişilerin niteliklerinin şeffaflığını, karşılaştırılabilirliğini ve taşınabilirliğini artırmaya yardımcı olur ve farklı ülke ve kurumlardan gelen niteliklerin karşılaştırılmasını mümkün kılar.

AYÇ, her tür ve her düzeydeki yeterlilikleri kapsar ve öğrenme kazanımlarının kullanımı, bir kişinin neyi bildiğini, anladığını ve yapabileceğini açıkça ortaya koyar. Seviye, yeterlilik seviyesine göre artar, seviye 1 en düşük, seviye 8 en yüksek seviyedir. En önemlisi, AYÇ ulusal yeterlilik çerçeveleriyle yakından bağlantılıdır, bu şekilde Avrupa'daki her tür ve düzeydeki yeterliliklerin kapsamlı bir haritasını sağlayabilir ve bu haritalara yeterlilik veri tabanları aracılığıyla giderek daha fazla erişilebilir.

AYÇ 2008 yılında kuruldu ve daha sonra 2017 yılında revize edildi. Revizyon, Avrupa'daki yeterlilikler ortamında şeffaflık ve karşılıklı güven yaratma temel hedeflerini korumuştur. Üye Devletler, AYÇ'yi daha da geliştirmeyi ve ulusal, uluslararası ve üçüncü ülke yeterliliklerinin işverenler, işçiler ve öğrenciler tarafından anlaşılmasını kolaylaştırmada daha etkili hale getirmeyi taahhüt ettiler.

AYÇ'nin 8 seviyesinin her biri, herhangi bir yeterlilik sisteminde o seviyedeki yeterliliklerle ilgili öğrenme kazanımlarını gösteren bir dizi tanımlayıcı ile tanımlanır. Öğrenme çıktıları şu şekilde tanımlanır:

- Bilgi: AYÇ bağlamında bilgi, teorik ve/veya olgusal olarak tanımlanır.
- Beceriler: AYÇ bağlamında beceriler bilişsel (mantıksal, sezgisel ve yaratıcı düşünmenin kullanımını içeren) ve pratik (el becerisi ve yöntemlerin, materyallerin, araçların ve araçların kullanımını içeren) olarak tanımlanmaktadır.
- Sorumluluk ve özerklik: AYÇ bağlamında sorumluluk ve özerklik, öğrencinin bilgi ve becerilerini özerk ve sorumlulukla uygulama yeteneği olarak tanımlanmaktadır.

**Masa 1-AYÇ Seviye-4 Öğrenme Çıktıları**

| Bilgi | Yetenek | Sorumluluk ve özerklik |
|---|---|---|
| Bir çalışma veya öğrenme alanındaki geniş bağlamlarda olgusal ve teorik bilgi | Bir iş veya eğitim alanındaki belirli sorunlara çözüm üretmek için gerekli olan bir dizi bilişsel ve pratik beceri | Öz yönetimi, genellikle öngörülebilir ancak değişikliğe tabi olan iş veya öğrenme bağlamlarının yönergeleri dahilinde uygulayın; başkalarının rutin çalışmalarını denetlemek, iş veya öğrenme etkinliklerinin değerlendirilmesi ve iyileştirilmesi için bazı sorumluluklar almak |

# 3. SIBER GÜVENLIK MESLEKI EĞITIM VE ÖĞRETIM ÖĞRENCILERI (EQF SEVIYE 4-5)

Siber Güvenlik çalışanı (Seviye 4-5), işyerinde bilgi sistemleri alanında çalışan, zafiyet takibi ve siber güvenlik farkındalık artırma süreçleri kapsamında siber güvenlik önleyici faaliyet çalışmalarına katılan, aksiyonları takip eden, siber güvenlik analizlerinde kullanılan sistemlerin işleyişini ve sürdürülebilirliğini izleyen, basit ağların gereksinimlerini belirleyen, nitelikli meslek elemanını, iş sağlığı ve güvenliği ile çevre koruma tedbirlerini uygulayarak kalite gereklilikleri çerçevesinde işyeri BT altyapılarının siber tehditlere karşı korunması için fiziksel ağlar kurar, ağ donanımı ile ilgili basit seviye konfigürasyonları gerçekleştirir, ağ güvenliğini, bakım ve iyileştirmelerini sağlar, kullanıcılara teknik destek sağlar ve mesleki gelişim çalışmaları yapar.

## 3.1. EQF-4-5 IÇIN CYBERAGENT LEARNING PROGRAMI

Mesleki Eğitim ve Öğretim müfredatı (EQF 4-5), kapsamlı HEI müfredatının (EQF 5-6) stratejik olarak uyarlanmasıyla geliştirilmiştir. Adaptasyon süreci, materyalin 1 AKTS kapsamına uygun olacak şekilde yoğunlaştırılmasını ve Mesleki Eğitim ve Öğretim hedef kitlesi ve acil KOBİ ihtiyaçları ile en alakalı öğrenme çıktılarına odaklanmayı içeriyordu. Pratik uygulama ve temel siber güvenlik becerilerini vurgulayan konulara öncelik verilirken, daha derinlemesine teorik kavramlar Mesleki Eğitim ve Öğretim öğrenme yoluna uyacak şekilde düzenlenmiştir.

**Masa 2-Modül: 1**

| Birimler | Konu |
|---|---|
| **Proje yönetimi** | Proje Planlaması<br>Proje Hedeflerinin Tanımlanması<br>Güncel Siber Güvenlik Tehditleri (DDoS, Ransomware, Kötü Amaçlı Yazılım, Phishing, Zero-Day, IoT saldırıları vb.) |

| | |
|---|---|
| | Tehdit Modelleme ve Zafiyet Analizi<br>Siber Güvenlik Tehditlerini ve Olaylarını Raporlama |
| Ders öğrenme kazanımları<br>• Öğrenciler proje yönetimi aşamalarını tanımlayabilecek ve temel bir proje planı oluşturabileceklerdir. (Uygulama)<br>• Öğrenciler açık, ölçülebilir ve ulaşılabilir proje hedeflerini ifade edeceklerdir. (Analiz)<br>• Öğrenciler çeşitli siber güvenlik tehditlerini tanımlayacak, sınıflandıracak ve değerlendirecektir. (Analiz)<br>• Öğrenciler, tehdit modelleri geliştirecek ve belirli senaryolar için güvenlik açığı analizleri gerçekleştireceklerdir. (Uygulama)<br>• Öğrenciler, belirlenmiş protokolleri izleyerek olay raporları hazırlayacaklardır. (Uygulama) | |
| **Kaynak yönetimi** | Güvenlik Araçları ve Yazılımları<br>Teknolojik Kaynakların Etkin Kullanımı |
| Ders öğrenme kazanımları<br>• Öğrenciler, tehdit tespiti ve müdahalesi için siber güvenlik araçlarının ve yazılımlarının etkili kullanımını göstereceklerdir. (Uygulama)<br>• Öğrenciler, gelişmiş güvenlik ve verimlilik için teknolojik kaynakları optimize edeceklerdir. (Uygulama) | |
| **Güvenlik ölçümleri** | Güvenlik Metrikleri ve Ölçüm Teknikleri<br>SIEM ile Veri Toplama<br>Güvenlik Metriklerinin Analizi<br>Proje İzleme ve Performans Değerlendirme<br>Güvenlik Metriklerinin Raporlanması |
| Ders öğrenme kazanımları<br>• Öğrenciler ilgili güvenlik ölçümlerini ve ölçüm tekniklerini belirleyecek ve uygulayacaktır. (Uygulama)<br>• Öğrenciler, veri toplama ve güvenlik izleme için SIEM araçlarını yapılandıracak ve kullanacaktır. (Uygulama)<br>• Öğrenciler, güvenlik duruşunu değerlendirmek için güvenlik ölçümlerini yorumlayacak ve analiz edeceklerdir. (Analiz)<br>• Öğrenciler, güvenlik ölçümlerini kullanarak proje performansını izleyecek ve değerlendirecektir. (Değerlendirme)<br>• Öğrenciler, güvenlik metrik analizine dayalı raporlar derleyecek ve sunacaktır. (Uygulama) | |
| **Kalite güvencesi ve kalite kontrol** | Kalite Yönetimi<br>Siber Güvenlikte Kalite Standartları<br>Test ve Doğrulama Teknikleri |
| Öğrenci çıktıları:<br>• Öğrenciler siber güvenlik projelerinde kalite yönetimi uygulamalarını uygulayacaklardır. (Uygulama)<br>• Öğrenciler ilgili siber güvenlik kalite standartlarını belirleyecek ve uygulayacaktır. (Uygulama)<br>• Öğrenciler, siber güvenlik çözümleri için test ve doğrulama prosedürleri geliştirecek ve yürütecektir. (Uygulama) | |

**Masa 3-Modül: 2**

| **Birimler** | **Konu** |
|---|---|
| **İşletim sistemi yönetimi** | İşletim Sistemleri<br>Donanım ve Yazılım Arasındaki İlişki<br>İkililer, Onaltılık Sayma<br>Bitler & Baytlar<br>İşletim sisteminde komut satırı<br>Windows & Linux Komutları<br>Windows İstemci & Sunucu<br>Windows'ta Uygulamalar, İşlemler ve Hizmetler<br>Dosya Uzantıları & Türleri<br>Kayıt Defteri Anahtarları ve Değerleri<br>Kontrol Paneli Ayarları<br>Kullanıcılar ve Gruplar<br>Domain Yapısı & Sunucu Yöneticisi<br>AD & GPO<br>Linux Arayüzleri & Çekirdek<br>Linux'ta Süreçler<br>Dosya & Dizin Adlandırma Kuralları<br>Linux Kabukları & Komut Sözdizimi<br>Dosya & Klasörleri Manipüle Etme<br>Boru & Sistem İzleme Komutları ile Çalışma<br>Süreç Yönetimi & İş Kontrolü<br>Servis Yönetimi |

Öğrenci çıktıları:

- Öğrenciler farklı işletim sistemlerini ve mimarilerini karşılaştıracak ve karşılaştıracaklardır.
- Öğrenciler, bir işletim sistemi ortamında donanım ve yazılım arasındaki etkileşimi açıklayacaklardır.
- Öğrenciler ikili ve onaltılık dönüşümler gerçekleştirecek ve veri temsilini anlayacaklardır.
- Öğrenciler, Windows ve Linux ortamlarında temel komutları çalıştıracaklardır.
- Öğrenciler, sistem araçlarını kullanarak uygulamaları, hizmetleri ve süreçleri yöneteceklerdir.
- Öğrenciler, Active Directory ve GPO'ları yapılandıracak ve yönetecektir.
- Öğrenciler Linux arayüzleriyle etkileşime girecek ve çekirdek düzeyinde işlemler gerçekleştireceklerdir.
- Öğrenciler, Linux komutlarını kullanarak hizmetleri ve sistem süreçlerini yöneteceklerdir.

| | |
|---|---|
| **Veritabanı sistemi yönetimi** | Depolar & Kaynak Listeleri<br>Web Sunucusunu Yönetme<br>Sistem Günlükleri & Günlük İzleme<br>Linux'ta Görevleri Zamanlama<br>Sunucu & Ağ Sorunları<br>Yedekleme & Kurtarma<br>GRUB'un Güvenliğini Sağlama<br>Güvenlik duvarları<br>Active Directory Nesneleri & GPO Yönetimi<br>DNS & DHCP<br>PowerShell Temelleri<br>Microsoft BitLocker, AppLocker & Güvenlik Duvarı<br>LDAP & Kerberos<br>NTLM Hakkında<br>Şifre & Kilitleme Politikaları<br>Kimlik Doğrulama & Erişim Kontrolü<br>İnternet Kontrol Mesajı Protokolü (ICMP)<br>TCP ve UDP karşılaştırması<br>NetBIOS & SMB<br>SSL & TLS<br>Sertifika<br>Telnet ve Secure Shell (SSH) Protokolleri<br>HTTP & HTTPS<br>Posta Sistemleri Protokolleri<br>Etki Alanı Adı Sistemi Protokolü (DNS)<br>FTP & RDP<br>Kapsülleme Vs. Dekapsülasyon<br>Ağ Sniffers & Wireshark<br>TCP/UDP<br>DHCP, DNS |
| Ders öğrenme kazanımları<br>• Öğrenciler depoları yapılandıracak ve kaynak listelerini yönetecektir.<br>• Öğrenciler, sorun giderme ve güvenlik için günlükleri analiz edecek ve izleyecektir.<br>• Öğrenciler, veri bütünlüğünü sağlamak için yedekleme ve kurtarma işlemleri gerçekleştirecektir.<br>• Öğrenciler güvenlik duvarları, BitLocker ve AppLocker gibi güvenlik önlemlerini uygulayacaktır. | |
| **Ağ yönetimi** | Ağ Türleri & Kablosuz Ağlar<br>Ağlar & Topolojiler<br>Cihazlar Kimlik & Erişim Cihazları<br>Altyapı & Güvenlik Cihazları<br>Özel Cihazlar & Ağ Mimarisi<br>Sanal Ağlar<br>Fiziksel ve Mantıksal Adresler<br>OSI & Ağ Modelleri<br>Veri Kapsülleme ve Kapsül Çıkarma<br>Ağ Protokolleri ve Bağlantı Noktası Numaraları<br>Ağ Ortamı ve Kabloları |

| | |
|---|---|
| | Kablosuz Teknolojiler<br>Ağ Yönetim Araçları<br>Cisco Paket İzleyici<br>Ağ Sınıfları & Alt Ağ Oluşturma<br>Adres Çözümleme Protokolü (ARP)<br>Statik ve Dinamik IP Adresleme<br>Ağ Adresi Çevirisi (NAT)<br>Anahtarlar & Cisco IOS<br>Switch Port Güvenlik & Router Arayüzleri<br>VLAN'ları ve DTP'yi yapılandırma<br>VLAN'lar Arası Yönlendirme<br>ACL'lere Giriş<br>Ağ Sorun Giderme |
| Ders öğrenme kazanımları<br>• Öğrenciler ağları tasarlayacak ve yönetecek, protokolleri ve topolojileri anlayacaklardır.<br>• Öğrenciler VLAN'ları, ACL'leri yapılandıracak ve IP adresleme şemalarını yönetecektir.<br>• Öğrenciler, izleme ve sorun giderme için Wireshark ve Cisco Packet Tracer gibi araçları kullanacaklardır. | |
| **Bulut yönetimi** | Hipervizörler & Sanal Makineler<br>Konteyner<br>Sanal Ortamların Güvenliğini Sağlama<br>Yedekleme & Kurtarma<br>Bulut Bilişim & CSP'ler<br>Bulut Hizmet Modelleri Nelerdir?<br>Bulut Dağıtım Türleri<br>Sanal Ağlar<br>AWS İşlem Hizmetleri<br>Amazon Esnek İşlem Bulutu (EC2)<br>Bulut İzleme Araçları<br>Otomasyon ve Orkestrasyon Araçları<br>Bulut Güvenliği Tehditleri ve Güvenlik Açıkları<br>Kimlik ve Erişim Yönetimi (IAM)<br>Rol Tabanlı Erişim Kontrolü (RBAC)<br>Çok Faktörlü Kimlik Doğrulama (MFA)<br>Bulut Veri Şifreleme<br>Sanal Özel Bulut (VPC)<br>Docker & Kubernetes |
| Ders öğrenme kazanımları<br>• Öğrenciler AWS, Docker ve Kubernetes kullanarak sanal ortamları yöneteceklerdir.<br>• Öğrenciler bulut güvenlik kontrollerini ve kimlik yönetimini uygulayacaktır. | |
| **Siber-fiziksel sistem yönetimi** | Güvenlik & Erişim Kontrolleri<br>Kimlik Doğrulama Türleri<br>TACACS+ ve RADIUS<br>AAA Yapılandırması<br>Risk Yönetimi Hedefleri<br>Şifreleme & Şifre Çözme<br>Hashing & Rainbow Tabloları<br>MAC Sahtekarlığı & ARP Zehirlenmesi |

| | |
|---|---|
| | VLAN Atlama & Rogue DHCP<br>ICMP Sel<br>TCP & UDP Sel<br>Oturum Ele Geçirme<br>DNS Sahtekarlığı<br>Derinlemesine Savunma (DID) & Sıfır Güven<br>Askerden Arındırılmış Bölgeler (DMZ'ler)<br>Bal Küpleri & Ağ Güçlendirme<br>Güvenli Bir Ağ için En İyi Uygulamalar<br>VPN'ler<br>SSH & VNC<br>Durum Bilgisi Olan ve Durum Bilgisi Olmayan Güvenlik Duvarları<br>Ana Bilgisayar Tabanlı ve Ağ Tabanlı<br>Donanım ve Yazılım Güvenlik Duvarları<br>Web Uygulaması Güvenlik Duvarı (WAF)<br>Güvenlik Duvarlarında Yapay Zeka<br>IDS & IPS<br>NIDS & HIDS<br>Snort<br>tcpdump |
| Ders öğrenme kazanımları<br>• Öğrenciler, güvenlik duvarları, IDS/IPS ve tehdit algılama araçlarını kullanarak ağların güvenliğini sağlayacaktır.<br>• Öğrenciler şifreleme tekniklerini uygulayacak ve güvenlik protokollerini yöneteceklerdir. | |
| **Sistem güçlendirme** | GenAI Teknikleri<br>Kod Oluşturma<br>Kullanıcı Hesabı Yönetimi ve Erişim Kontrolü<br>Anomali Tespiti ve Sorun Giderme<br>Apache2 Hizmet Hatalarını Çözme<br>Yama Yönetimi & Güncellemeler<br>Otomatik Yedekleme & Kurtarma<br>GenAI ile Silinen Dosyaları Kurtarma<br>Siber Güvenlik Prosedürleri<br>Tehdit Tespiti & Analizi<br>Tehdit Yanıtı ve İyileştirme<br>Gerçek Zamanlı Tehdit Tespiti için Yapay Zekadan Yararlanma<br>GenAI Modellerinin Doğrulanması ve Test Edilmesi<br>DNS Yapılandırma & Güvenlik<br>DHCP Yapılandırma & Güvenlik<br>PowerShell Temelleri<br>Anahtar Bağlantı Noktası Güvenliği<br>Ağ Temel Giriş/Çıkış Sistemi (NetBIOS)<br>Sunucu İleti Bloğu Protokolü (SMB)<br>Güvenli Yuva Katmanı (SSL) & Taşıma Katmanı Güvenliği (TLS)<br>Güvenlik Sertifikaları<br>Posta Sistemleri Protokolleri |

| | |
|---|---|
| | Etki Alanı Adı Sistemi Protokolü (DNS)<br>Dosya Aktarım Protokolü (FTP)<br>Uzak Masaüstü Protokolü (RDP)<br>Linux'ta Görevleri Zamanlama<br>Sunucu Sorun Giderme<br>Ağ Sorun Giderme<br>Yedekleme & Kurtarma<br>GRUB'un Güvenliğini Sağlama<br>Güvenlik Duvarlarını Kurma & Güvence Altına Alma |
| Ders öğrenme kazanımları<br>• Öğrenciler, sistem güvenliğini artırmak için sertleştirme tekniklerini uygulayacaklardır.<br>• Öğrenciler, tehdit tespiti ve sistem izleme için yapay zekadan yararlanacak. | |
| **Sistem güçlendirme** | IR ve SOC<br>Olaylar ve Olaylar<br>Uyarı Tespiti & Uyarı Triyajı<br>Dokümantasyon ve Raporlama<br>Web Saldırıları Nedir?<br>DoS ve DDoS<br>SQL Enjeksiyonu & XSS<br>Komut Enjeksiyonu & Yerel Dosya Dahil Etme (LFI)<br>Siteler Arası İstek Sahteciliği (CSRF)<br>Brute-Force & Credential Stuffing<br>Hash'i Geç & Bileti Geç<br>Bozuk Erişim Kontrolü<br>Fidye yazılımı<br>Bilgisayar Virüsü & Solucanı<br>Truva Atı & Reklam Yazılımı<br>Keylogger & Cryptojacking<br>Dosyasız Kötü Amaçlı Yazılım<br>Kötü Amaçlı Yazılımın Yayılmasını Anlamak<br>IOC'leri ve Şifre Politikalarını Yönetme<br>Kabul Edilebilir Kullanım İlkeleri (AUP)<br>Kendi Cihazını Getir (KCG) Politikaları<br>Uzaktan Erişim İlkeleri |
| Ders öğrenme kazanımları<br>• R ve SOC'nin kilit rollerini ve işbirliğini ayırt edin.<br>• Güvenlik olayları ve ihlaller arasındaki farkı tanımlayın.<br>• Güvenlik uyarılarının kaynaklarını ve önceliklendirme işlemlerini açıklayın.<br>• Güvenlik olayları için etkili dokümantasyon ve raporlama sağlayın.<br>• Yaygın web saldırısı türlerini (DoS/DDoS, SQL Enjeksiyonu, XSS, Komut Enjeksiyonu, LFI, CSRF) ana hatlarıyla belirtin.<br>• Kaba kuvvet ve kimlik bilgisi doldurma saldırılarını açıklayın ve karşı önlemlerini ana hatlarıyla belirtin.<br>• "Hash'i geç" ve "bileti geç" saldırılarının temel ilkelerini anlayın.<br>• Bozuk erişim kontrolü güvenlik açıklarından nasıl yararlanılabileceğini açıklayın.<br>• Farklı kötü amaçlı yazılım türlerini (Fidye Yazılımı, Virüs, Solucan, Truva Atı, Reklam Yazılımı, Keylogger, Cryptojacking, Dosyasız Kötü Amaçlı Yazılım) ve yayılma yöntemlerini açıklayın. | |

| |
|---|
| • Tehdit istihbaratı göstergelerini (IOC'ler) yönetmenin önemini açıklayın.<br>• Güçlü parola politikalarının ve kabul edilebilir kullanım politikalarının (AUP'ler) temel unsurlarını ana hatlarıyla belirtin.<br>• BYOD ve uzaktan erişim politikalarının güvenlik etkilerini değerlendirin. |

**Masa 4-Modül: 3**

| **Birimler** | **Konu** |
|---|---|
| **Performans ölçümleri (metrikler)** | Performans Metrikleri<br>Sistem ve Ağ İzleme<br>Performans Metriklerini İzleme<br>Ağ Haritalama<br>Güvenlik Açığı Taraması<br>Ağ Trafiği Analizi |
| Ders öğrenme kazanımları<br>• Öğrenciler performans ölçütlerini tanımlayacak ve bunların sistem ve ağ performansını değerlendirmedeki önemini açıklayacaklardır.<br>• Öğrenciler, sistem ve ağ performansının sürekli değerlendirilmesi için izleme araçlarının kurulumunu ve kullanımını göstereceklerdir.<br>• Öğrenciler, sistem sağlığını değerlendirmek ve optimizasyon fırsatlarını belirlemek için performans ölçümlerini analiz edecek ve yorumlayacaktır.<br>• Öğrenciler, ağ yapılarını görselleştirmek, izlemek ve optimize etmek için ağ haritaları oluşturacaktır.<br>• Öğrenciler güvenlik açığı taramaları yapacak, güvenlik risklerini belirleyecek ve iyileştirme adımları önerecektir.<br>• Öğrenciler, potansiyel tehditleri tespit etmek ve bunlara yanıt vermek için ağ trafiği analizi yapacaklardır. | |
| **Veri analitiği** | Veri koleksiyonu<br>Veri Temizleme ve Ön İşleme<br>Veri Analizi<br>Veri Görselleştirme<br>Analitik Araçlar<br>Siber Güvenlikte Veri Analitiği Uygulamaları |
| Ders öğrenme kazanımları<br>• Öğrenciler, analiz için sistemlerden, ağlardan ve güvenlik günlüklerinden ilgili verileri toplayacaktır.<br>• Öğrenciler, doğruluk ve tutarlılığı sağlamak için ham verileri temizleyecek ve ön işleme tabi tutacaktır.<br>• Öğrenciler, verilerden anlamlı içgörüler elde etmek için istatistiksel ve analitik teknikleri uygulayacaklardır.<br>• Öğrenciler, analiz sonuçlarını etkili bir şekilde iletmek için veri görselleştirmeleri oluşturacaklardır.<br>• Öğrenciler kapsamlı veri analizi için Python, R ve Power BI gibi araçları kullanacaklardır. | |

| | |
|---|---|
| • Öğrenciler, siber güvenlik tehditlerini tespit etmek, analiz etmek ve azaltmak için veri analitiği tekniklerini uygulayacaklardır. | |
| **Güvenlik istihbaratı** | Güvenlik İstihbaratını Anlamak<br>Güvenlik İstihbaratının Kaynakları<br>Tehdit İstihbaratı Toplama Yöntemleri<br>Güvenlik İstihbaratı Uygulamalarına İlişkin Örnek Olay İncelemeleri |
| Ders öğrenme kazanımları<br>• Öğrenciler, proaktif tehdit yönetiminde güvenlik istihbaratının önemini açıklayacaklardır.<br>• Öğrenciler, tehdit akışları, raporlar ve açık kaynaklı araçlar dahil olmak üzere güvenlik istihbaratı kaynaklarını değerlendireceklerdir.<br>• Öğrenciler, tehdit istihbaratı toplama ve analiz etme yöntemlerini tanımlayacaklardır.<br>• Öğrenciler, siber tehditleri önlemede güvenlik istihbaratının uygulanmasını anlamak için gerçek dünyadaki vakaları inceleyeceklerdir. | |

**Masa 5-Modül: 4**

| **Birimler** | **Konu** |
|---|---|
| **Güvenlik Operasyonlarının temelleri** | Güvenlik Operasyonlarını ve SOC'yi (Güvenlik Operasyonları Merkezi) Anlamak<br>Güvenlik Operasyonlarındaki roller ve sorumluluklar<br>Güvenlik operasyonları araçlarına ve teknolojilerine genel bakış<br>Pratik örnekler ve vaka çalışmaları |
| Ders öğrenme kazanımları<br>• Öğrenciler, bir Güvenlik Operasyon Merkezinin amacını ve yapısını ve siber güvenlikteki rolünü açıklayacaklardır.<br>• Öğrenciler, olay müdahalesi, tehdit avcılığı ve izleme dahil olmak üzere güvenlik operasyonları personelinin rollerini ve sorumluluklarını açıklayacaklardır.<br>• Öğrenciler, ortak güvenlik operasyonları araçlarının ve teknolojilerinin kullanımını tanımlayacak ve göstereceklerdir.<br>• Öğrenciler, uygulamadaki güvenlik operasyonlarını anlamak için gerçek dünyadan örnekleri ve vaka çalışmalarını analiz edeceklerdir. | |
| **Güvenlik Yakınsaması** | Güvenlik yakınsamasını anlama<br>Fiziksel güvenliğin temelleri (fiziksel güvenlik ilkeleri, fiziksel varlıkların korunması, politikalar)<br>KOBİ'lerin karşılaştığı yaygın tehditler<br>Yakınsama sorunlarını vurgulayan vaka çalışmaları |
| Ders öğrenme kazanımları<br>• Öğrenciler güvenlik yakınsamasını tanımlayacak ve fiziksel ve siber güvenlik önlemlerinin entegrasyonundaki önemini açıklayacaklardır.<br>• Öğrenciler, varlıkları, tesisleri ve personeli korumak için fiziksel güvenlik ilkelerini uygulayacaklardır.<br>• Öğrenciler, küçük ve orta ölçekli işletmelerin (KOBİ'ler) yaygın olarak karşılaştığı güvenlik tehditlerini belirleyecek ve değerlendireceklerdir. | |

| | |
|---|---|
| • Öğrenciler, yakınsama zorluklarının etkisini anlamak için vaka çalışmalarını inceleyeceklerdir.<br>• Öğrenciler güvenlik bilgilerini ve etkinlik yönetimi süreçlerini gözden geçireceklerdir. | |
| **Güvenlik Bilgileri ve Olay Yönetimi** | Güvenlik izleme ilkelerinin gözden geçirilmesi (diğer ortaklar modülüne dayalı)<br>SIEM çözümlerini uygulama<br>Günlükleri ve uyarıları ayarlama<br>Tehdit istihbaratı ve algılama metodolojilerinin gözden geçirilmesi (diğer ortaklar modülüne göre) |
| Ders öğrenme kazanımları<br>• Öğrenciler, güvenlik izleme ilkelerini ve bunların SIEM çözümlerindeki uygulamalarını açıklayacaklardır.<br>• Öğrenciler, etkili tehdit algılama ve yanıt için SIEM çözümlerini yapılandıracak ve çalıştıracaktır.<br>• Öğrenciler, güvenlik olaylarını izlemek için SIEM araçlarında günlüğe kaydetme ve uyarı mekanizmaları kuracaktır.<br>• Öğrenciler, etkili güvenlik operasyonları için tehdit istihbaratı ve tespit metodolojilerini değerlendireceklerdir. | |
| **Güvenlik Operasyonları Uygulamaları** | Uyumluluk ve düzenleme<br>Güvenlik operasyonlarında sürekli iyileştirme stratejileri<br>Otomasyon ve orkestrasyon<br>Metrikler ve raporlama |
| Ders öğrenme kazanımları<br>• Öğrenciler, güvenlik operasyonlarında uyum ve düzenlemenin önemini açıklayacaklardır.<br>• Öğrenciler, güvenlik operasyonları için sürekli iyileştirme stratejileri tasarlayacak ve uygulayacaktır.<br>• Öğrenciler, güvenlik operasyonlarının verimliliğini artırmak için otomasyon ve orkestrasyondan yararlanacaktır.<br>• Öğrenciler, güvenlik duruşunu iletmek için güvenlik ölçümleri ve raporlama teknikleri geliştirecek ve kullanacaklardır. | |

**Masa 6-Modül: 5**

| **Birimler** | **Konu** |
|---|---|
| **Organizasyonel bağlam** | KOBİ'lerde siber güvenliğin evrimi<br>Mevcut büyük tehditler ve güvenlik açıkları<br>Siber güvenliğin iş stratejisine etkisi<br>KOBİ'lerde büyük işletmelere karşı siber güvenliğin belirli zorlukları<br>Siber güvenlik uygulamalarının düzenleyici etkilerini ve bunların yönetişim yapılarıyla nasıl uyumlu olduğunu anlayın.<br>Sınırlı bütçeler, özel güvenlik personelinin eksikliği ve siber güvenlik yatırımlarına öncelik vermek için pratik yöntemler gibi KOBİ'lere özgü siber güvenlik zorluklarını karşılayın. |
| Ders öğrenme kazanımları | |

<table>
<tr><td colspan="2">

- Öğrenciler, küçük ve orta ölçekli işletmelerde siber güvenlik uygulamalarının gelişimini izleyeceklerdir.
- Öğrenciler, KOBİ'leri etkileyen en kritik mevcut tehditleri ve güvenlik açıklarını belirleyecek ve değerlendirecektir.
- Öğrenciler, siber güvenliğin iş stratejisini ve operasyonel karar almayı nasıl etkilediğini analiz edeceklerdir.
- Öğrenciler, KOBİ'lerin karşılaştığı siber güvenlik zorluklarını daha büyük kuruluşların karşılaştığı zorluklarla karşılaştıracaktır.
- Öğrenciler, siber güvenlik için düzenleyici gereklilikleri yorumlayacak ve bunların kurumsal yönetişimle nasıl bütünleştiğini değerlendireceklerdir.
- Öğrenciler, bütçe kısıtlamaları ve sınırlı personel gibi yaygın KOBİ siber güvenlik sorunlarına yönelik pratik çözümleri açıklayacaklardır.

</td></tr>
<tr><td>Gizlilik</td><td>Siber güvenlikte gizlilik ilkeleri<br>Kişisel verilerin korunması ve GDPR<br>Gizliliğin KOBİ operasyonları üzerindeki etkisi<br>Gizliliğin korunmasına yönelik araçlar ve teknikler</td></tr>
<tr><td colspan="2">Ders öğrenme kazanımları

- Öğrenciler, siber güvenlik bağlamında temel gizlilik ilkelerini açıklayacaklardır.
- Öğrenciler GDPR gerekliliklerini uygulayacak ve bunların kişisel verilerin korunması üzerindeki etkilerini değerlendirecektir.
- Öğrenciler, gizlilik düzenlemelerinin KOBİ'lerin günlük operasyonlarını ve iş modellerini nasıl etkilediğini değerlendireceklerdir.
- Öğrenciler, gizliliği korumak ve hassas verileri korumak için araçlar kullanacak ve teknikler uygulayacaktır.

</td></tr>
<tr><td>Yasalar, etik ve uyumluluk</td><td>Siber Güvenlik Kuruluşları, Politikaları ve Standartları<br>İlgili ulusal ve uluslararası mevzuat<br>KOBİ'lerde mevzuata uygunluk<br>Siber Güvenlikte Etik<br>Siber güvenlikte uyumsuzluğun hukuki sonuçları<br>Siber güvenlik yönetişimini güçlendirmek ve sürekli izleme ve otomatik tehdit yanıtı yoluyla uyumluluğu sağlamak için yapay zeka tabanlı araçların nasıl kullanılabileceğinin analizi.</td></tr>
<tr><td colspan="2">Ders öğrenme kazanımları

- Öğrenciler önemli siber güvenlik kuruluşlarını belirleyecek ve ilgili politika ve standart çerçevelerini değerlendireceklerdir.
- Öğrenciler, ulusal ve uluslararası düzeyde siber güvenliği etkileyen temel yasaları özetleyeceklerdir.
- Öğrenciler, KOBİ bağlamlarında mevzuat uyumluluğunu sağlamak ve sürdürmek için stratejiler tasarlayacaklardır.
- Öğrenciler siber güvenlik karar verme ve davranışlarındaki etik hususları inceleyeceklerdir.
- Öğrenciler, siber güvenlik yasalarına uymamanın yasal sonuçlarını değerlendireceklerdir.
- Öğrenciler, yapay zeka araçlarının yönetişimi nasıl iyileştirebileceğini, izlemeyi nasıl otomatikleştirebileceğini ve uyumluluğu nasıl geliştirebileceğini keşfedecekler.

</td></tr>
<tr><td>Güvenlik idaresi</td><td>Siber güvenlik yönetişim yapısı<br>Güvenlik yönetiminde rol ve sorumluluklar</td></tr>
</table>

| | |
|---|---|
| | Siber güvenlik olgunluk modelleri<br>Simüle edilmiş kriz koşulları altında risk değerlendirmeleri yapma ve stratejik müdahale planları oluşturma becerilerini geliştirin (Fidye yazılımı, kimlik avı saldırısı, ..)<br>Yönetici ve yönetim kurulu düzeyinde iletişim<br>Siber güvenlik iletişim stratejileri<br>Üst yönetime güvenlik raporlaması<br>Siber güvenlikte kriz yönetimi ve iletişim<br>Yapay zeka odaklı saldırılar ve fidye yazılımları içeren yüksek stresli senaryolarda kriz yönetimi ve karar verme becerilerinde uzmanlaşın. |
| Ders öğrenme kazanımları<br>• Öğrenciler, etkili siber güvenlik yönetimini destekleyen yönetişim yapılarını tasarlayacak ve değerlendireceklerdir.<br>• Öğrenciler, kurumsal güvenlik çerçevelerinde sorumlulukları atayacak ve netleştirecektir.<br>• Öğrenciler, yerleşik modelleri kullanarak siber güvenlik olgunluğunu değerlendireceklerdir.<br>• Öğrenciler, fidye yazılımı veya kimlik avı gibi senaryolar için risk değerlendirmeleri yapacak ve yanıt stratejileri geliştireceklerdir.<br>• Öğrenciler, siber güvenlik içgörülerini üst düzey yöneticilere ve yönetim kurulu üyelerine iletmek için iletişim planları geliştireceklerdir.<br>• Öğrenciler, iç ve dış siber güvenlik paydaşları için etkili iletişim stratejileri formüle edeceklerdir.<br>• Öğrenciler, üst yönetimi siber güvenlik performansı ve riskleri hakkında bilgilendiren raporlar oluşturacaktır.<br>• Öğrenciler, yapay zeka odaklı saldırıları içerenler de dahil olmak üzere siber güvenlik krizleri sırasında yönetme ve iletişim kurma pratiği yapacaklardır | |
| **Yönetim politikası** | Politika uygulama ve izleme |
| Ders öğrenme kazanımları<br>• Öğrenciler siber güvenlik politikalarını uygulayacak ve bunların sürekli izlenmesi ve uygulanması için prosedürler oluşturacaktır. | |

**Masa 7-Modül: 6**

| **Birimler** | **Konu** |
|---|---|
| **Siber Güvenlik Planlamasına Giriş: Veri, insan ve toplumsal güvenlik** | Veri güvenliği - Bilgi Depolama Güvenliği, Soruşturma süreci<br>Veri güvenliği - Parola saldırısı teknikleri<br>İnsan güvenliği -Farkındalık ve anlayış<br>Toplumsal güvenlik – Siber Suçlar nedir, Siber etik<br>Toplumsal güvenlik - Siber hukuk- Dijital deliller, Dijital sözleşmeler, Çok uluslu sözleşmeler (anlaşmalar) |
| Ders öğrenme kazanımları<br>• Öğrenciler, saklanan bilgileri güvence altına almak ve soruşturma süreçlerini desteklemek için stratejiler uygulayacaklardır. | |

<table>
<tr><td colspan="2">
<ul>
<li>Öğrenciler, yaygın parola saldırı tekniklerini belirleyip analiz edecek ve uygun karşı önlemler geliştireceklerdir.</li>
<li>Öğrenciler siber güvenlik farkındalığını artıracak ve çalışanlar ile paydaşlar arasında anlayışı geliştirecektir.</li>
<li>Öğrenciler siber suçların toplumsal sonuçlarını açıklayacak ve dijital ortamlardaki etik hususları değerlendireceklerdir.</li>
<li>Öğrenciler, dijital kanıtlar, sözleşmeler ve uluslararası anlaşmalar dahil olmak üzere temel siber hukuk kavramlarını yorumlayacaklardır.</li>
</ul>
</td></tr>
<tr><td>Operasyonel ve Taktik Yönetim</td><td>Erişim Kontrollerinin Uygulanması<br>Yama Yönetimi ve Yazılım Güncellemeleri<br>Sürekli Sistem İzleme<br>Çalışan Güvenliği Farkındalık Eğitimi</td></tr>
<tr><td colspan="2">Ders öğrenme kazanımları
<ul>
<li>Öğrenciler, sistemleri ve verileri korumak için etkili erişim kontrol mekanizmaları tasarlayacak ve uygulayacaktır.</li>
<li>Öğrenciler, güvenlik açıklarını azaltmak için zamanında yama yönetimi ve yazılım güncellemeleri için prosedürler oluşturacaktır.</li>
<li>Öğrenciler, güvenlik olaylarını tespit etmek ve bunlara yanıt vermek için sistemleri sürekli olarak izleyeceklerdir.</li>
<li>Öğrenciler, çalışan katılımını artırmak ve insan riskini azaltmak için güvenlik farkındalığı eğitim programları geliştirecek ve sunacaktır.</li>
</ul>
</td></tr>
</table>

**Masa 8-Modül: 7**

| **Birimler** | **Konu** |
|---|---|
| **Risk değerlendirmesi** | Genel risk yönetimi çerçevesi ve süreci<br>Risk yönetimi ilkeleri<br>Risk yönetimi standartları<br>Pratik örnekler ve vaka çalışmaları |
| Ders öğrenme kazanımları<br>• Öğrenciler, siber güvenlikte risk yönetiminin genel çerçevesini ve sürecini tanımlayacak ve uygulayacaktır.<br>• Öğrenciler, etkili siber güvenlik risk yönetimine rehberlik eden temel ilkeleri açıklayacaklardır.<br>• Öğrenciler, yaygın olarak kabul edilen risk yönetimi standartlarını belirleyecek ve yorumlayacaktır.<br>• Öğrenciler, gerçek dünyadan örnekler ve vaka çalışmaları aracılığıyla risk senaryolarını değerlendireceklerdir | |
| **Risk tanımlama** | Maddi ve manevi risk kaynakları<br>Nedenler ve olaylar<br>Tehditler ve fırsatlar<br>Güvenlik açıkları ve yetenekler<br>Dış ve iç bağlamdaki değişiklikler<br>Ortaya çıkan risklerin göstergeleri<br>Varlıkların ve kaynakların doğası ve değeri<br>Sonuçlar ve hedefler üzerindeki etkileri<br>Bilginin sınırlılıkları ve bilginin güvenilirliği<br>İlgili kişilerin önyargıları, varsayımları ve inançları.<br>Pratik örnekler ve vaka çalışmaları. |
| Ders öğrenme kazanımları<br>• Öğrenciler, siber güvenlik ortamlarında somut ve soyut risk kaynakları arasında ayrım yapacaklardır.<br>• Öğrenciler risk nedenlerini ve tetikleyici olayları belirleyeceklerdir.<br>• Öğrenciler siber güvenlik tehditlerini analiz edecek ve iyileştirme için potansiyel fırsatları değerlendireceklerdir.<br>• Öğrenciler, riskleri yönetmedeki güvenlik açıklarını ve organizasyonel yetenekleri değerlendireceklerdir.<br>• Öğrenciler bağlamsal değişikliklerin siber güvenlik risklerini nasıl etkilediğini değerlendireceklerdir.<br>• Öğrenciler, yeni siber güvenlik tehditlerinin ortaya çıktığına işaret eden göstergeleri belirleyeceklerdir.<br>• Öğrenciler, riskle ilişkili olarak varlık değerini ve kaynak kritikliğini değerlendireceklerdir.<br>• Öğrenciler potansiyel sonuçları ve bunların stratejik hedefler üzerindeki etkilerini tahmin edeceklerdir.<br>• Öğrenciler, risk tanımlama sürecindeki bilgi ve bilginin sınırlamalarını fark edeceklerdir.<br>• Öğrenciler, insan faktörlerinin risk algısını ve tanımlamasını nasıl etkilediğini yansıtacaklardır. | |

| | |
|---|---|
| • Öğrenciler, gerçek dünya senaryoları aracılığıyla tanımlama tekniklerini uygulayacaklardır. | |
| **İçeriden gelen tehditler** | İçeriden gelen tehditlerin tanımı ve türleri<br>İçeriden gelen tehditleri tespit etme ve tanımlama<br>Pratik örnekler ve vaka çalışmaları |
| Ders öğrenme kazanımları<br>• Öğrenciler içeriden gelen tehditleri tanımlayacak ve çeşitli türleri sınıflandıracaktır.<br>• Öğrenciler, içeriden gelen tehdit göstergelerini tespit etme ve bunlara yanıt verme becerilerini geliştireceklerdir.<br>• Öğrenciler, gerçek hayattaki içeriden tehdit olaylarına ilişkin vaka çalışmalarını analiz edeceklerdir. | |
| **Risk ölçme ve değerlendirme modelleri ve metodolojileri** | Nicel ve nitel risk değerlendirme modelleri ve metodolojileri<br>Olayların olasılığı ve sonuçları<br>Sonuçların niteliği ve büyüklüğü<br>Hassasiyet ve güven seviyeleri.<br>Pratik örnekler ve vaka çalışmaları |
| Ders öğrenme kazanımları<br>• Öğrenciler, siber güvenlik risk değerlendirmelerinde hem nicel hem de nitel modelleri karşılaştıracak ve uygulayacaktır.<br>• Öğrenciler, belirlenen risklerin olasılığını ve potansiyel sonuçlarını değerlendireceklerdir.<br>• Öğrenciler, siber güvenlik riskleriyle ilişkili sonuçların ciddiyetini ve kapsamını değerlendireceklerdir.<br>• Öğrenciler, risk değerlendirmelerinde belirsizlik ve güven düzeylerini belirleyeceklerdir.<br>• Öğrenciler risk değerlendirme modellerini pratik senaryolarda uygulayacaklardır. | |
| **Risk kontrolü** | İzleme ve inceleme<br>Kayıt ve raporlama<br>Pratik örnekler ve vaka çalışmaları |
| Ders öğrenme kazanımları<br>• Öğrenciler düzenli risk izleme ve gözden geçirme süreçleri yürüteceklerdir.<br>• Öğrenciler risk kontrol önlemlerini etkili bir şekilde belgeleyecek ve raporlayacaktır.<br>• Öğrenciler, etkili risk kontrolü uygulamasını anlamak için gerçek dünyadan örnekleri inceleyeceklerdir. | |

**Masa 9-Modül: 8**

| **Birimler** | **Konu** |
|---|---|
| **Olay yanıtı** | Olay Müdahalesinin Tanımı ve Önemi<br>Etkili Bir Olay Müdahale Kurtarma Planının Temel Bileşenleri<br>Yaygın Siber Güvenlik Tehditleri |
| Ders öğrenme kazanımları<br>• Öğrenciler olay müdahalesini tanımlayacak ve siber güvenlik yönetimindeki önemini açıklayacaklardır.<br>• Öğrenciler, yapılandırılmış bir olay müdahale kurtarma planının temel unsurlarını belirleyecek ve uygulayacaktır. | |

| | |
|---|---|
| • Öğrenciler, olay yönetimi sırasında karşılaşılan yaygın siber güvenlik tehditlerini tanıyacak ve bunlara yanıt verecektir. | |
| **Olağanüstü durum kurtarma** | Felaket Kurtarmayı Anlamak<br>Felaket Kurtarma'daki roller ve sorumluluklar<br>Felaketten sonra kurtarma adımları |
| Ders öğrenme kazanımları<br>• Öğrenciler, siber güvenlik bağlamında felaket kurtarmanın ilkelerini ve hedeflerini açıklayacaklardır.<br>• Öğrenciler, felaket kurtarmada yer alan ekip üyelerinin rollerini ve sorumluluklarını tanımlayacaklardır.<br>• Öğrenciler, bir siber felaketten sonra sistemleri ve operasyonları geri yüklemek için adım adım bir plan geliştireceklerdir. | |
| **İş sürekliliği** | İş sürekliliğini anlamak<br>İş sürekliliğinde rol ve sorumluluklar<br>İş Etki Analizi |
| Ders öğrenme kazanımları<br>• Öğrenciler iş sürekliliği planlaması kavramını ve önemini açıklayacaklardır.<br>• Öğrenciler, iş sürekliliğinin sağlanmasıyla ilgili rol ve sorumlulukları belirleyeceklerdir.<br>• Öğrenciler, kritik işlevleri ve bağımlılıkları değerlendirmek için bir iş etki analizi yapacaklardır. | |
| **Güvenlik bilinci, eğitim ve öğretim** | Güvenlik farkındalığını anlamak<br>Siber güvenlikte çalışan sorumlulukları |
| Ders öğrenme kazanımları<br>• Öğrenciler, insan kaynaklı siber güvenlik risklerini azaltmada güvenlik farkındalığının rolünü açıklayacaklardır.<br>• Öğrenciler, siber güvenlik protokollerini ve en iyi uygulamaları sürdürme konusunda çalışanların sorumluluklarını tanıyacaklardır. | |
| **Güvenlik işe alma uygulamaları** | Güvenlik rolleri gereksinimlerini tanımlama<br>Geçmiş kontrolleri boyunca yürütmek |
| Ders öğrenme kazanımları<br>• Öğrenciler siber güvenlik iş rollerini tanımlayacak ve uygun gereksinimleri formüle edeceklerdir.<br>• Öğrenciler, güvenlik açısından hassas roller için geçmiş kontrolleri yaparken en iyi uygulamaları uygulayacaktır. | |
| **Güvenlik sonlandırma uygulamaları** | Erişimi hemen iptal etme<br>İlgili ekiplerin bilgilendirilmesi<br>Yasal ve uyumluluk hususları |
| Ders öğrenme kazanımları<br>• Öğrenciler, çalışanın işten çıkarılması üzerine erişimi derhal iptal etmek için prosedürler uygulayacaktır.<br>• Öğrenciler, işten ayrılma sürecinde ilgili departmanlarla iletişimi koordine edeceklerdir.<br>• Öğrenciler, siber güvenlikte iş akdinin feshi ile ilgili yasal ve uyumluluk gerekliliklerini inceleyeceklerdir. | |
| **Üçüncü taraf güvenliği** | Üçüncü taraf riskinin değerlendirilmesi<br>Karşıtlıkların ve güvenlik gereksinimlerinin uygulanması |

| | |
|---|---|
| | Sürekli izleme ve denetim<br>Olay müdahalesi ve iletişim |
| Ders öğrenme kazanımları<br>• Öğrenciler, üçüncü taraf satıcılar ve ortaklarla ilişkili güvenlik risklerini değerlendirecektir.<br>• Öğrenciler, üçüncü taraf güvenlik uyumluluğunu sağlamak için sözleşme maddelerini tasarlayacak ve uygulayacaktır.<br>• Öğrenciler, üçüncü taraf güvenliği için sürekli izleme ve denetim uygulamaları oluşturacaktır.<br>• Öğrenciler, olay müdahale faaliyetleri sırasında üçüncü taraflarla koordinasyon sağlayacaktır. | |
| **İnceleme süreçlerinde güvenlik** | Gözden geçirmelere güvenlik ekleme<br>Güvenlik açığı değerlendirmesi ve sızma testi<br>Olay sonrası incelemeler |
| Ders öğrenme kazanımları<br>• Öğrenciler, güvenlik hususlarını kurumsal inceleme süreçlerine entegre edeceklerdir.<br>• Öğrenciler, gözden geçirme etkinliklerinin bir parçası olarak güvenlik açığı değerlendirmeleri ve sızma testleri yapacaklardır.<br>• Öğrenciler, etkinliği değerlendirmek ve gelecekteki yanıtları iyileştirmek için olay sonrası incelemeler yapacaklardır. | |
| **Çalışanların kişisel bilgilerinin gizliliğine ilişkin özel sayı** | Veri toplama sınırlamaları<br>Depolama ve erişim kontrolü<br>Gizlilik düzenlemelerine uygunluk<br>Veri paylaşımı ve üçüncü taraflar<br>Çalışan onayı ve hakları |
| Ders öğrenme kazanımları<br>• Öğrenciler, çalışanların kişisel verilerini toplamak için uygun sınırları belirleyecektir.<br>• Öğrenciler, hassas çalışan verileri için güvenli depolama ve erişim kontrolü önlemleri uygulayacaktır.<br>• Öğrenciler, GDPR gibi ilgili gizlilik düzenlemelerine uyumu sağlayacaktır.<br>• Öğrenciler, çalışan verilerinin üçüncü taraflarla paylaşılmasıyla ilgili riskleri ve kuralları değerlendirecektir.<br>• Öğrenciler, çalışan haklarını ve bilgilendirilmiş onam almanın önemini anlayacaklardır. | |

## SON

Bu rapor, CyberAgent eğitiminin başarılı bir şekilde uygulanması için dikkate alınması gereken mesleki eğitim düzeyine uygun müfredatı sunmaktadır. Projenin başlangıcından bu yana eğitim ihtiyaçlarını belirlemek için yapılan araştırmaların ardından, bu belge mesleki eğitim öğrencilerinin katılımlarına yönelik ihtiyaçlarını açıklamaktadır.

Programın hazırlanması sırasında CyberAgent projesi EQF Seviye 5-6 için hazırlanan müfredat referans alınmıştır. Bu seviye müfredatından AYÇ Seviye 4-5'e uygun konular seçilmiştir.

Son olarak, eğitimin içerik, organizasyon ve beceri geliştirme açısından en yüksek kalitede olmasını sağlamak amacıyla, AYÇ Düzey 5-6'dan aktarılmayan konularla ilgili sorular.

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