CyberAgent

Co-funded by the European Union

KOBİ SIBER GÜVENLIK DEĞIŞIM AJANLARI ÖĞRENME YOLUNUN YAPISI

SIBER AJAN 06.2024

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

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

İş Paketi 2: CyberAgent yaklaşımı ve yapı tasarımı

Çıktı 2.3: KOBİ Siber Güvenlik Değişim Ajanları öğrenme yolunun yapısı

WP2 Lideri – Olemisen Balanssia ry
Teslim edilebilir 2.3 Lideri – Vilnius Üniversitesi

İÇERİK

KISALTMA

CBL – Meydan Okumaya Dayalı Öğrenme Modeli

CL – İşbirlikli Öğrenme Modeli

EC – Avrupa Komisyonu

AKTS – Avrupa Kredi Transfer ve Biriktirme Sistemi

AYÇ – Avrupa Yeterlilikler Çerçevesi

GICL – Rehberli Sorgulama İşbirlikçi Öğrenme Modeli

HEI – Yükseköğretim Kurumları

PDÖ – Proje Tabanlı Öğrenme Modeli

POGIL – Süreç Odaklı Rehberli Sorgulama Öğrenme Modeli

KOBİ – Küçük ve Orta Ölçekli İşletmeler

VET – Mesleki Eğitim Kurumları

ŞEKİLLER LİSTESİ

TABLOLARIN LISTESI

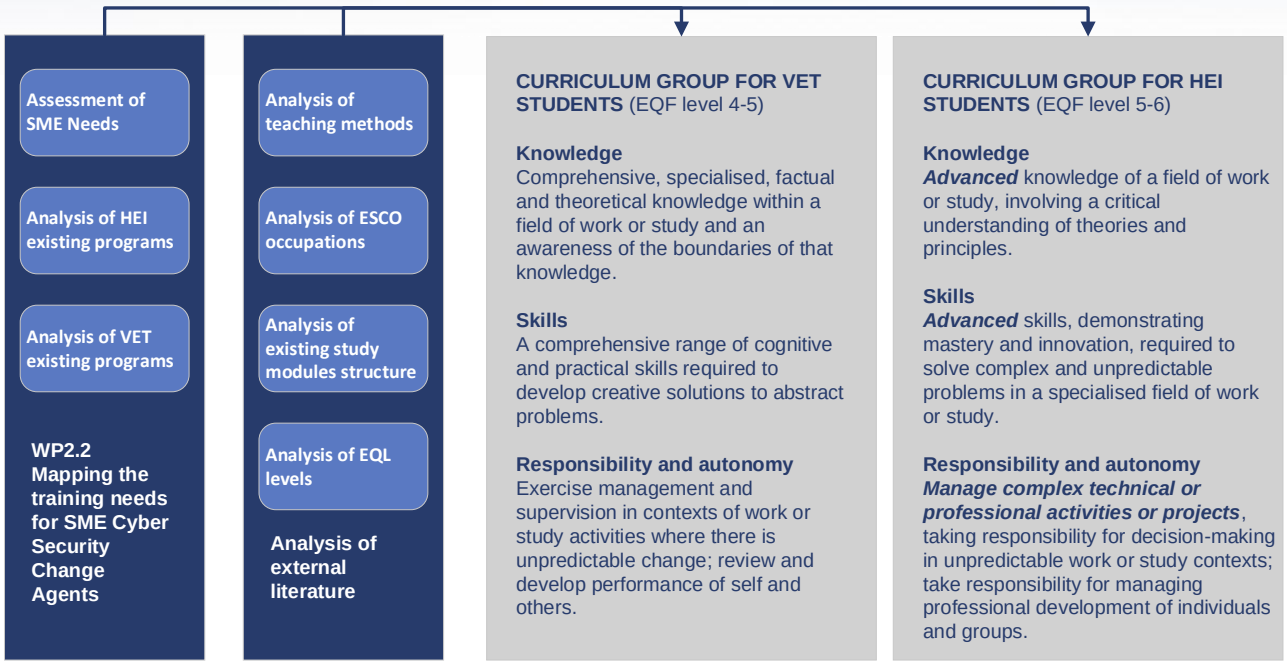
GIRIŞ

Bu raporun genel amacı, Avrupalı KOBİ (Küçük ve Orta Ölçekli İşletmeler) çalışanları arasında siber güvenlik becerilerini geliştirmek için yeni profesyonel öğrenme yolları geliştirmek ve tanımlamaktır.

KOBİ Siber Güvenlik Değişim Ajanları için eğitim ihtiyaçlarının haritalandırılmasından elde edilen bulgulara dayanarak, öğrenme çıktılarının bilgi, beceri ve yetkinlikler açısından dış kaynak analizi belirlenmiştir. Belirlenen öğrenme kazanımlarının analizinin ardından, bu rapor, proje hedef grupları, KOBİ çalışanları ve öğrencileri için gerekli olan bilgi ve beceri yelpazesini kapsayacak ve eğitim çıktılarını kursiyerlerin farklı geçmişlerine ve profillerine uyarlayacak şekilde AYÇ (Avrupa Yeterlilikler Çerçevesi) seviye 4'ten 6'ya kadar iki tür eğitim müfredatı hakkında rehberlik sağlar.

- EQF seviye 4-5, mesleki eğitim ve mesleki eğitim (mesleki eğitim ve öğretim) çalışmalarının yanı sıra yükseköğretim geçmişi olmayan KOBİ çalışanları için de uygulanacaktır. Bu seviye, bazı modüllerde hafif uzmanlaşma ile siber güvenlik temel becerilerini ve bilgilerini sağlayacaktır.
- EQF seviye 5-6, takip etmek için yeterli altyapıya sahip KOBİ çalışanları ve HEI (Yükseköğretim Kurumları) öğrencileri için bir teklif olacaktır. Bu seviyede, daha ileri ve karmaşık eğitim faaliyetleri gerçekleştirilecektir.

AYÇ seviyelerinin sadece daha önce belirtildiği gibi geniş bir öğrenme çıktısı yelpazesini kapsayacak şekilde değil, aynı zamanda Mesleki Eğitim ve Öğretim öğrencileri ve 4. seviyedeki çalışanlar için 6. seviyeye ulaşmaları için bir beceri geliştirme yolu olarak eğitim müfredatları arasında bir geçit sağlamak için 4-6 olarak güncellenmesine karar verildi.



Şekil 1. EC yönergelerine bağlı kalan açıklayıcı bir diyagram, eğitim çerçevesinin görsel bir temsilini sağlayan sekiz AYÇ seviyesini tasvir etmektedir.[1]

Müfredat, öğrenme çıktılarını ve KOBİ Çalışanlarının KOBİ Siber Güvenlik Değişim Ajanları rolünü doldurmak için kendilerini geliştirmeleri ve yükseköğretim ve mesleki eğitim öğrencilerini eğitimden sonra rolü doldurmaları için eğitmeleri için eğitim ihtiyacını ele almaktadır. Her müfredat, dört alt konuyu kapsayan sekiz modülden oluşur:

- Teknik beceriler - Siber güvenlik tehditleri ve ilgili yasal konular hakkında güncellenmiş bilgiler - Siber güvenlik tehditleriyle nasıl başa çıkılacağına dair pratik bilgiler.
- Analitik beceriler - Eleştirel düşünme zihniyeti - Yerel tehditleri, nasıl meydana geldiklerini, risk altındaki insanları vb. analiz etme ve anlama becerisi.
- Risk yönetimi - KOBİ işyerlerine siber güvenlik rutinleri sağlamayı ve tanımlamayı öğrenin - Siber güvenlik için kendi işyeri KOBİ el kitabınızı ve bunu nasıl takip edeceğinizi öğrenin.
- Organizasyon becerileri - KOBİ işyerlerinde siber güvenlikte yeni rutinlerin ve çalışma yöntemlerinin nasıl uygulanacağı; Siber güvenlik konusunda lider desteği yürütmek.

Buna ek olarak, Avrupalı KOBİ'ler arasında siber güvenlik becerilerinin geliştirilmesine yönelik öğrenme yollarının oluşturulmasının merkezi bir parçası, mikro kimlik bilgilerinin nasıl uygulanacağıdır. Öğrenme çıktılarına (bilgi, beceri ve yetkinlikler), ders içeriğine, eğitime (bilgi, beceri ve yetkinlikler), oyunlaştırma unsurlarına, süreye ve AKTS sayısına (Avrupa Kredi Transfer ve Biriktirme Sistemi) atıfta bulunmaları gerekir. Amaca uygun olması için, yükseköğretim kurumları ile Mesleki Eğitim ve Öğretim sağlayıcıları ve siber güvenlik sektöründen özel işletmeler arasında ortaklıklar kurulması yoluyla teslim edilmeleri gerekir.

[1] https://europa.eu/europass/en/description-eight-eqf-levels

Mikro bölümler, öğrencilere modülleri veya modüllerin bölümlerini seçme ve hangi sertifika seviyesine ihtiyaç duyduklarına karar verme konusunda daha fazla özgürlük sağlar: katılım sertifikaları veya sertifika testli kurs bitirme sertifikası, yani kursun belirli bir yetkinliğin kazanılmasıyla tamamlandığının kanıtı. Kurs bitirme sertifikaları, final sınavını en az %75 puanla geçmek için verilir ve belirli konularda/modüllerde yüz yüze, harmanlanmış öğrenme veya çevrimiçi eğitime katılmak için katılım sertifikaları verilir. Bu uygulama sadece eğitimin uygulanabilirliğini ve etkinliğini artırmakla kalmaz, aynı zamanda öğrenme motivasyonunu teşvik ederek katılımcıların kariyerleri ve daha fazla gelişimi için net bir değer perspektifi sağlar.

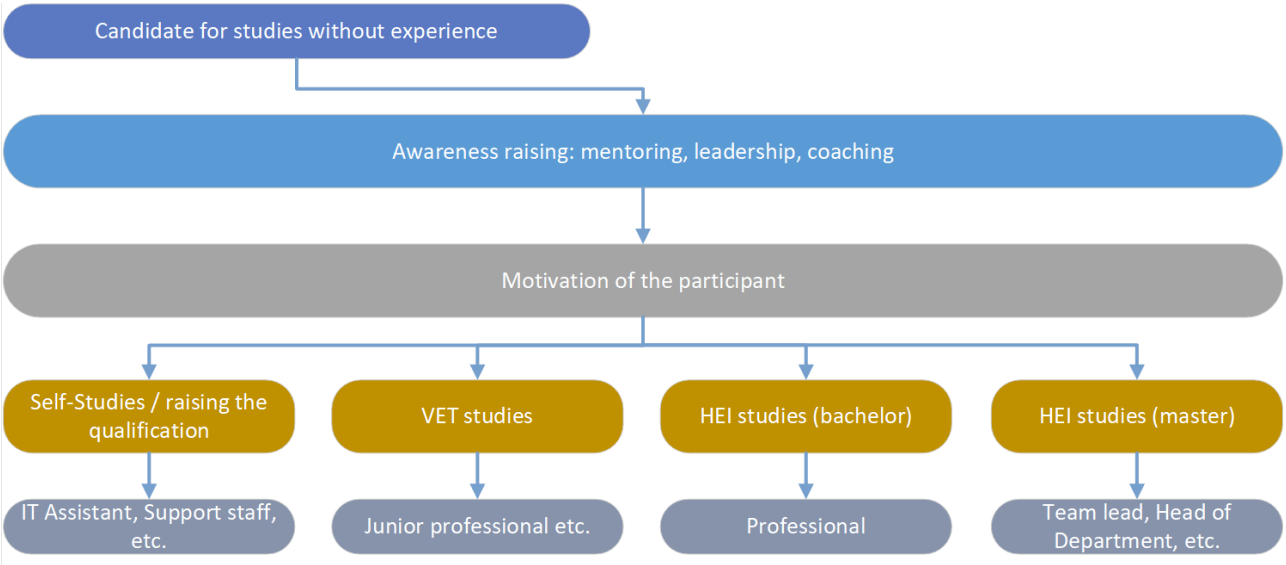
Genel olarak, bu rapor, çalışma ve taşıyıcı yollarının içerik taslağı, eğitim ve değerlendirme metodolojileri ve müfredat oluşturma yol haritası dahil olmak üzere CyberAgent modüllerinin geliştirilmesi için ayrıntılı kılavuzları özetlemektedir.

1. ÇALIŞMA YOLU

Öğrenme yolu, katılımcının becerilerini geliştirmesi, eğitime başlaması ve tamamlaması gerektiğini fark ettiği andan, öğrenmeyi bitirdiği ve edindiği bilgileri uygulamaya başladığı ana kadar yaptığı bütün bir yolculuktur. Bir öğrenme yolunda 3 aşama vardır:

- Ön öğrenme,
- Öğrenme
- Öğrenme sonrası.

Ön öğrenme aşaması aşağıdaki şekilde gösterilmiştir.



Şekil 2. Çalışmalar başlamadan önce öğrenme yolu

KOBİ'ler bağlamında, bu öğrenme/çalışma yolu takip edilebilir. Şekilde, katılımcı ya kendini eğitmeye karar verir ya da bir bilinçlendirme kampanyasından etkilenir ve eğitimin faydaları, fırsatlar ve eğitimden sonra edinilebilecek kariyerler hakkında bir anlayış kazanır.

OLE (Çevrimiçi Öğrenme Ortamı) yapısı aracılığıyla tipik bir modül olarak öğrenme yolu da önerilmiştir. Literatür taraması ve mikro-kimlik ilkeleri ilkesini uygulayan birkaç projeden sonra[2,3,4], her bir CyberAgent modülünün 1-5 AKTS (her AKTS 25-30 saatlik iş yükü) olması önerilmekte ve bir giriş ile başlanmakta ve daha sonra alt konular olan temalara ayrılmaktadır.

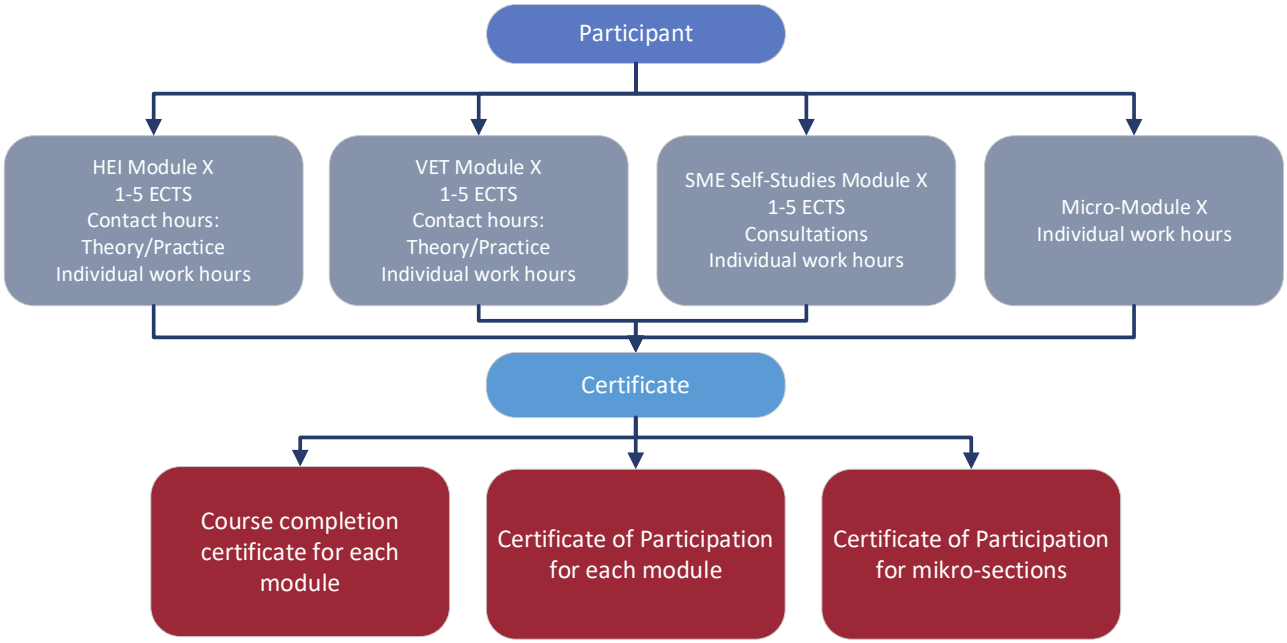
Konuların sonunda birkaç sorudan oluşan bir öz değerlendirme testi yapılır. Modülün eğitim materyalleri, her birinde 4-6 alt konu bulunan 6-8 konunun çalışılmasını desteklemelidir. Kurs,

[2] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Eğitimde İleri ve Öteye Gitmek: ESNEK ÖĞRENME YOLLARI kavramı. KTÜ leidykla "Technologija" e-Kitaplarında. https://doi.org/10.5755/e01.9786090218204

[3] https://arqus-alliance.eu/call/arqus-microcredential-development-f2f-workshop/

[4] https://www.youtube.com/watch?v=ECH0VvHIyRI, https://ndma.lt/alta2023/

zorunlu olmayan bir bilgi testi ile sona erebilir. Bu, KOBİ çalışanlarına ve eğitim kurumlarının öğrencilerine, eğitimin belirli bir modülünde veya bölümünde öğrenilen yeterlilikleri edinme ve gösterme imkanı verir.



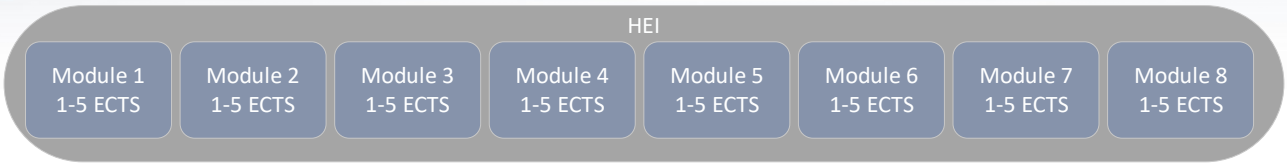
Şekil 3. Çalışmaların yapısı

Mikro kimlik bilgileri, aşağıdaki temel faaliyetler aracılığıyla öğrenme sürecine entegre edilir:

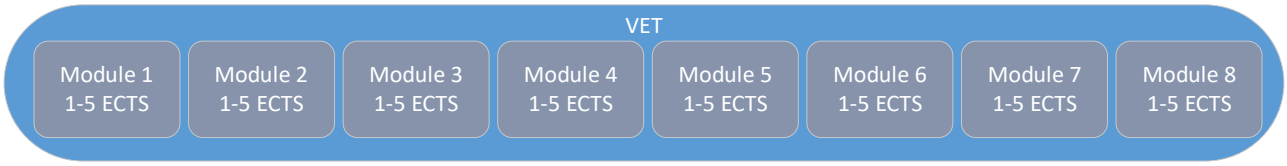
- Eğitim modüllerinin geliştirilmesi: Her modül, KOBİ sektöründe gerekli olan özel bilgi ve beceriler dikkate alınarak, net hedefler, öğrenme çıktıları, öğretme ve öğrenme yöntemleri, kurs süresi ile dikkatli bir şekilde formüle edilmelidir.
- Pratik görevler ve projeler: öğrenciler pratik görevleri yerine getirir ve değerlendirilen ve edinilen becerilerin net kanıtını sağlayan projeler geliştirir.
- Açıkça tanımlanmış bilgi değerlendirme stratejisi ve değerlendirme kriterleri: Her modülün sonunda, katılımcının gerekli öğrenme çıktılarına ulaşıp ulaşmadığını ve bunu kanıtlamak için bir sertifika almaya uygun olup olmadığını belirlemek için bir bilgi değerlendirmesi düzenlenir.

Projenin hedef grubu KOBİ çalışanları, yükseköğretim ve mesleki eğitim ve öğretim öğrencileri olduğundan, öğrencilerin olanaklarına ve ihtiyaçlarına göre dört tür çalışma mevcuttur:

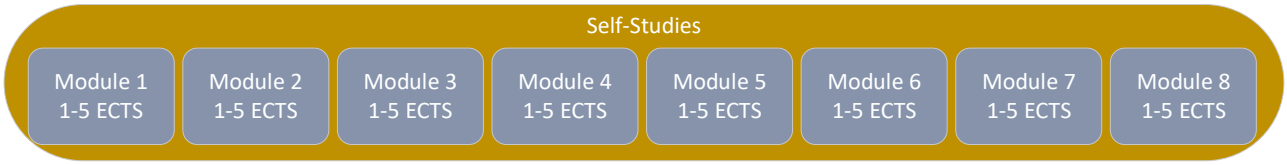
- HEI çalışmaları: her biri 1-5 AKTS'lik 8 modül, temas saatleri (teori ve pratik) ve bireysel çalışma saatleri vardır;
- Mesleki Eğitim ve Öğretim çalışmaları: Her biri 1-5 AKTS'lik 8 modül, temas saatleri (teori ve pratik) ve bireysel çalışma saatleri vardır;
- Kendi Kendine Çalışmalar (KOBİ'ler için): Her biri 1-5 AKTS'lik 8 modül, burada istişareler (gerekirse) ve bireysel çalışma saatleri vardır;
- Mikro modüller: seçilen konuların sayısına bağlı olarak bireysel çalışma saatleri.



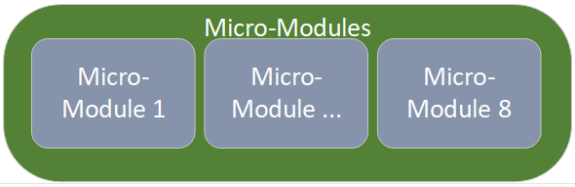
Şekil 4. HEI için çalışma yapısı



Şekil 5. Mesleki Eğitim ve Öğretim için çalışma yapısı

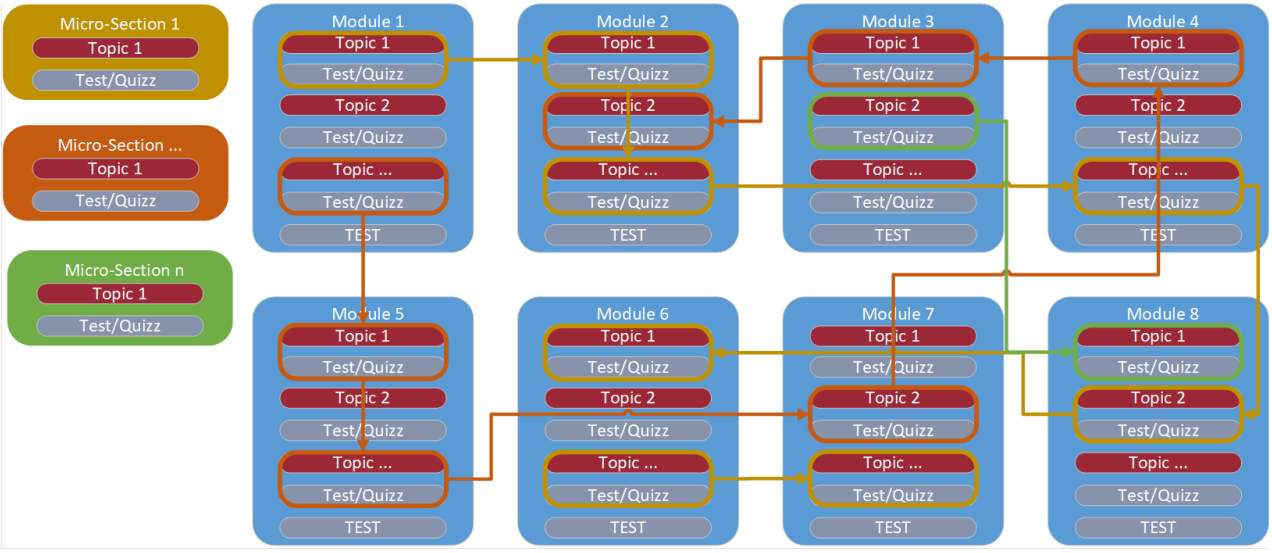


Şekil 6. Kendi Kendine Çalışmalar için çalışma yapısı



Şekil 7. Mikro modülün yapısını inceler

HEI ve VET öğrencileri, her biri 1-5 kredilik bir modül çalışabilecekler. KOBİ'ler her seferinde bir modül alabilecek veya kursun bir parçası olarak mikro kesitler sunabileceğiz.



Şekil 8. Öğrenme yolları bağlantıları

Her üç öğrenme türünde de (HEI, Vet, KOBİ'ler) öğrenci 8 modül çalışır. Mikro modüller söz konusu olduğunda, öğrenci modülleri kendi seçimine göre seçer. Esc

Mikro modüller, kısa veya uzun, şeffaf bir şekilde değerlendirilen öğrenme deneyimleridir. Katılımcı tarafından meydan okuma ile birlikte veya ayrı ayrı alınırlar. Her mikro modül, farklı miktarda öğrenme iş yükü ölçüsü (AKTS gibi) ile değerlendirilir ve değerlendirme ile tamamlanır. Mikro modül değerlendirmesinin başarıyla tamamlanması, öğrencileri mikro kimlik bilgileriyle ödüllendirir.

Öneri, HEI programındaki her modülün, her biri özel ödevler ve ayrıntılı bir uygulama planı içeren tek bir mikro modüle modüler hale getirilebilmesidir. Test sonuçları, görüntü tabanlı ve bilgisayarlar tarafından evrensel olarak okunabilen rozetler aracılığıyla değerlendirilebilir. Bu görüntülerde, her bir rozetle ilişkili yetkinlikleri detaylandıran meta veriler ve rozete sahip olan katılımcı hakkında bilgiler yer alır.

Mikro kimlik bilgisi, bir katılımcının küçük bir öğrenme hacminin ardından edindiği öğrenme kazanımlarının kaydı anlamına gelir. Bu öğrenme çıktıları şeffaf ve açıkça tanımlanmış kriterlere göre değerlendirilecektir. Mikro kimlik bilgilerine yol açan öğrenme deneyimleri, katılımcıya toplumsal, kişisel, kültürel veya işgücü piyasası ihtiyaçlarına cevap veren belirli bilgi, beceri ve yetkinlikler sağlamak için tasarlanmıştır [5,6].

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Eğitimde İleri ve Öteye Gitmek: ESNEK ÖĞRENME YOLLARI kavramı. KTÜ leidykla "Technologija" e-Kitaplarında. https://doi.org/10.5755/e01.9786090218204

[6] 16 Haziran 2022 tarihli Konsey Tavsiye Kararı, Yaşam Boyu Öğrenme ve İstihdam Edilebilirlik için Mikro Kimlik Bilgilerine Avrupa Yaklaşımı." Avrupa Birliği Resmi Gazetesi, cilt 2022/C, 16 Haziran 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=TR

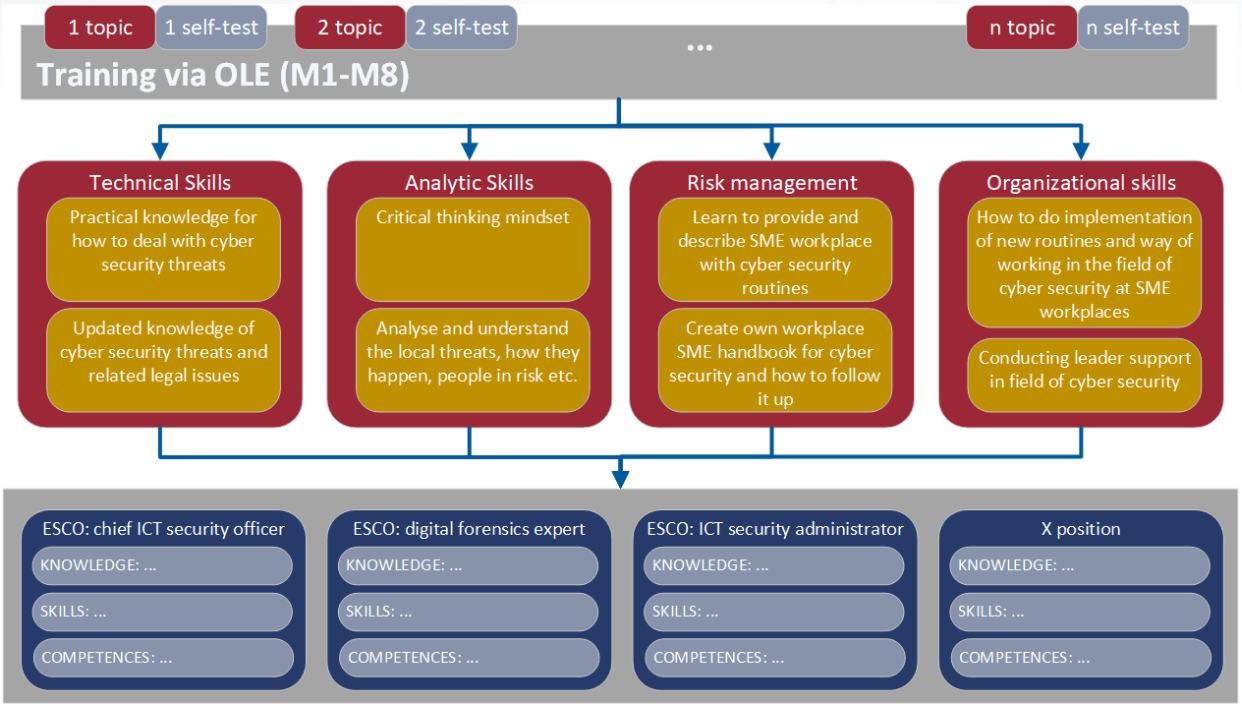
2. TAŞIYICI YOLU

Öğrenme sonrası yol, taşıyıcı yol olarak adlandırılabilir. Projenin başlangıcında, ESCO mesleklerinin araştırma analizi yapıldı (Raporda açıklanmıştır: D2.2 - KOBİ Siber Güvenlik Değişim Ajanları Eğitimi İhtiyaç Haritalama Raporu). Üç aşamada gerçekleştirilen analiz, ESCO çerçevesinde listelenen çeşitli siber güvenlik mesleklerini araştırmayı amaçladı. İlk aşamada, siber güvenlikle ilgili meslekler belirlendi ve **ESCO portalından** belgelenerek ilgili becerileri, yetkinlikleri ve bilgileri vurgulandı. Bu meslekler, baş BİT güvenlik görevlisi, dijital adli tıp uzmanı, gömülü sistem güvenlik mühendisi, etik bilgisayar korsanı, BİT esneklik yöneticisi, BİT güvenlik yöneticisi, BİT güvenlik mühendisi, BİT güvenlik yöneticisi ve bilgi mühendisi gibi rolleri içeriyordu. Her meslek, kurumsal güvenlik işlevlerinden dijital adli tıp, etik bilgisayar korsanlığı ve dayanıklılık planlamasına kadar siber güvenlik alanındaki belirli sorumlulukları ve odak alanları ile tanımlandı.

İkinci aşamada, incelenen her ESCO mesleği için, unvanını ve temel sorumluluklarını detaylandıran bir tablo dolduruldu. Bunlar, güvenlik önlemlerinin planlanması ve uygulanması, güvenlik açığı değerlendirmelerinin yapılması, dayanıklılık ve felaket kurtarma için modeller geliştirilmesi ve bilgilerin bilgisayar sistemlerine entegre edilmesi gibi görevleri içeriyordu.

Ek olarak, üçüncü aşama, ESCO mesleklerinin ilgili öğrenme çıktılarıyla haritalandırılmasını ve bunların bilgi, beceri ve yeterliliklere göre kategorize edilmesini içeriyordu. Bu süreç, her bir siber güvenlik rolü için eğitim gereksinimlerinin ve beklenen yeterliliklerin kapsamlı bir şekilde anlaşılmasını kolaylaştırarak endüstri standartları ve en iyi uygulamalarla uyum sağladı. Bu aşamalar boyunca analiz, daha sonraki araştırmalar için değerli bilgiler sağladı.

Şekil 9. Önceki raporda tanımlanan ESCO meslekleri



Şekil 10. Olası Öğrenme sonrası yollar

Şekil 10, OLE (Çevrimiçi öğrenme ortamı) (HEI, VET, SME) yoluyla çalışmaların tamamlanmasından ve ESCO meslekleriyle uyumlu becerilerin kazanılmasından sonra izlenebilecek potansiyel kariyer yollarını göstermektedir.

Kariyer fırsatlarının daha net bir şekilde anlaşılmasıyla, siber güvenlik eğitimi alan HEI ve VET öğrencileri, kariyer seçeneklerini daha net bir şekilde anlayacak ve daha ileri bir çalışma alanı seçebilecek veya belirli pozisyonlardaki şirketlerde çalışabilecekken, BT ve diğer öğrenciler CyberAgent modüllerini bireysel çalışma modülleri olarak seçebilecek, böylece çalışma alanı yeterliliklerini geliştirebilecek, organizasyon ve risk yönetimi becerileri vb.

KOBİ personeli, işyeri yeterliliklerini geliştirme ve geliştirme fırsatına sahip olacak. Geliştirilen kariyer yoluna ve net kariyer fırsatlarına dayanarak, diğer KOBİ personeli siber güvenlik alanında yeniden eğitim alabilecektir.

Mentorluk programlarının entegrasyonu, yaygınlaştırma etkinliklerinin organizasyonu, atölye çalışmaları (proje, tüm ortaklar tarafından düzenlenen 6 ortak çalıştayın yanı sıra her ortak tarafından düzenlenen yaygınlaştırma kampanyalarını içerir), iş ve siber güvenlik temsilcilerinin davet edilmesi, sosyal ortaklar ve CyberAgent ağı ile işbirliği, öğrencilere staj imkanı sunulması, ve saire. Ayrıca, hedefli sosyal yardım ve destek programları da dahil olmak üzere çeşitlilik girişimlerimiz, kapsayıcı bir siber güvenlik iş gücünü teşvik ederek kadınların katılımını artırmayı amaçlıyor.

Katılımcılar, ESCO mesleklerini CyberAgent eğitim modüllerimizle kapsamlı bir şekilde eşleştirerek, öğrenme ortamlarından siber güvenlikte etkili rollere sorunsuz bir şekilde geçiş yapabilirler. CyberAgent kursiyerlerinin kariyer gelişimlerini takip etmek için eğitim öncesi, eğitim sonrası ve 3 aylık eğitim sonrası anketler düzenleyerek becerilerinin çalıştıkları kurumların siber

güvenliğine nasıl katkı sağladığını ortaya çıkarması planlanmaktadır. Anketler eğitim platformuna entegre edilecek ve kursun başlangıcından önce, kursun sonunda, ilerlemeyi ölçmek ve kursu ve eğitimin kalitesini değerlendirmek için kursiyerlere otomatik olarak sunulacaktır. Katılımcıların kariyerlerinde herhangi bir değişiklik olup olmadığını öğrenmek için üçüncü bir anket kullanılacaktır.

3. ÖĞRETIM YÖNTEMLERI

Vilnius Üniversitesi'nin (VU) Bilgi Sistemleri ve Siber Güvenlik çalışma programının, Timtal ve Moisil Buzau çalışma programlarının ve dış literatürün pedagojik yöntemlerinin analizi, öğretim yöntemlerinin birkaç yenilikçi kombinasyonunu önermemizi sağlar. Bu kombinasyonlar, her modülün yapısı dikkate alınarak çalışma modüllerine dahil edilebilir.[7]

Masa 1. Önerilen öğretim yöntemleri

Kategori	Detaylı bilgi
Anlatım ve doğrudan öğretim	- **Teorik dersler:** temel kavramlar ve teoriler. - **Konuk konuşmacılar** ((sertifikalı uzmanlar: Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı (CISSP), Sertifikalı Bilgi Sistemleri Denetçisi (CISA), Sertifikalı Bilgi Güvenliği Yöneticisi (CISM), CompTIA Security+, Sertifikalı Etik Hacker (CEH), GIAC Güvenlik Temelleri Sertifikası (GSEC), Sistem Güvenliği Sertifikalı Uygulayıcı (SSCP), CompTIA Gelişmiş Güvenlik Uygulayıcısı (CASP+), GIAC Sertifikalı Olay İşleyicisi (GCIH), Saldırgan Güvenlik Sertifikalı Profesyonel (OSCP))).

Pratik ve uygulamalı öğrenme	- **Pratik Görevler/Laboratuvarlar:** uygulamalı deneyler ve pratik alıştırmalar.
	- **Uygulamalı Etkinlikler**: gerçek dünya uygulamaları ve etkileşimli görevler.
	- **Teknik Video Analizi:** teknik becerilerin öğrenilmesi için video içeriğinin analizi.
	- **Simüle Edilmiş Ortamlar**:
	  o Bulut ortamı için barındırılan makineler.
	  o Hedef makineye saldırılar başlatın.
	  o Saldırıları planlamak ve gerçekleştirmek için makine – bir saldırı kutusu.

Ölçme ve değerlendirme	- **Sınavlar, Oyunlar, Yapılması ve Yapılmaması Gerekenler**: İlgi çekici ve etkileşimli değerlendirmeler.

[7] Siber Güvenlik Öğretimi: Proje Tabanlı Öğrenme ve Rehberli Sorgulama İşbirlikçi Öğrenme Yaklaşımı https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

Kategori	Detaylı bilgi
	- **Öz Değerlendirme Testleri**: Konuların sonunda öğrencinin öz değerlendirmesi için.
Bireysel çalışmalar	- **Kendi kendine rehberli öğrenme:** Bu yöntem, kişiselleştirilmiş öğrenme yollarını destekler ve öğrencilerin gerektiğinde erişebilecekleri dijital kaynaklar ve modüler içerikle geliştirilebilir.
İşbirlikçi ve akran öğrenimi	- **İşbirlikçi Öğrenme, Takım Çalışması**: grup projeleri ve işbirlikçi görevler. - **Eşler Arası öğretme ve öğrenme**: öğrenciler birbirlerinden öğretir ve öğrenirler. - **Grup mentorluğu ve/veya bireysel mentorluk**: daha deneyimli kişiler tarafından sağlanan rehberlik.
Teknolojiyle geliştirilmiş öğrenme	- **Oyunlaştırılmış siber güvenlik öğrenme platformunun kullanımı**: öğrenme platformlarındaki oyun benzeri öğeler aracılığıyla öğrencilerin ilgisini çekmek. - **Bayrağı ele geçirme yarışmaları**: siber güvenlik becerilerini geliştirmek için rekabetçi etkinlikler. - **Yarışmalar**: Yarışmalar, öğrencilerin bilgi ve becerilerini pratik, uygulamalı bir ortamda test eder ve rekabetçi bir formatta yeterliliklerinin bir ölçüsünü sağlar.
Topluluk ve halk katılımı	- **Eğitim etkinlikleri:** Siber Güvenlik Ayı gibi girişimler sırasında özel etkinlikler. - **Halka açık sunumlar**: seminerler, konferanslar ve web seminerleri. - **Sosyal ağ**: öğrenme ve katılım için sosyal medya ve ağların kullanımı. - **Gündüz Kampüsü**: tipik olarak atölye çalışmaları, konferanslar ve ağ oluşturma fırsatlarını içerebilen sürükleyici, kampüs tabanlı etkinlikleri içerir
Yenilikçi öğrenme modelleri	- **BSCS 5E Öğretim Modeli (5E)** – 5E, aşağıdakilerden oluşan aşağıdaki aşamalara

Kategori	Detaylı bilgi
	odaklanır: Katılım, Keşif, Açıklama, Detaylandırma, Değerlendirme. - **Meydan Okumaya Dayalı Öğrenme Modeli (CBL) – CBL'** nin erken bir uygulaması, altı aşamadan oluşan bir çerçeve sağlar: Zorluğu tanımlayın, Fikirlerin üretilmesi ve beyin fırtınası yapılması, sorgulayan ve destekleyen çoklu bakış açılarını gözden geçirin, En iyi çözümler için araştırma yapın ve gözden geçirin, Hipotezi test edin, Bulguları ve sonuçları paylaşın. - **İşbirlikli Öğrenme Modeli (CL)** – 5E ve CBL modellerine benzer şekilde, İşbirlikli Öğrenme küçük gruplar halinde aktif öğrenmeyi teşvik eder ve öğrenciler performanslarına göre bir not, sertifika veya burs gibi somut bir ödül veya bir öğretmenin onayını içerebilecek bir ödül alırlar. - **Proje Tabanlı Öğrenme Modeli (PDÖ)** – Proje Tabanlı Öğrenme ve Probleme Dayalı Öğrenme, PBL'nin aynı kısaltmasını kullanır ve her ikisi de problem çözme, eleştirel düşünme, takım çalışması, iletişim ve yaratıcı becerileri geliştirmeye odaklanır; ancak, farklı aşamalardan oluşurlar., Bağımsız ve grup araştırması, Geliştirme ve sunma, Süreci analiz etme ve değerlendirme. - **Süreç Odaklı Rehberli Sorgulama Öğrenme Modeli (POGIL)** – bu yaklaşım, öğrencilere bir kavramın keşfi yoluyla rehberlik eder; ardından öğrencilerin kavramı sentezlediği ve açıkladığı kavram buluşu; ve teorik kavramın uygulanmasıyla öğrenme döngüsünü kapatır. - **Rehberli Sorgulama İşbirlikçi Öğrenme Modeli (GICL)** – bu, büyük ölçüde POGIL modeline dayanan yeni bir yaklaşımdır.

Sunulan çeşitli eğitim stratejilerinin mümkün olan en iyi etkiye sahip olmasını sağlamak için, kapsamlı bir modül müfredatı ve eğitim materyallerinin geliştirilmesinde her yaklaşım seçilecek ve siber güvenlik modüllerinin özel öğrenme hedefleriyle uyumlu hale getirilecektir. CyberAgent eğitimini verecek olan öğretim görevlileri/mentorlar tarafından ek yöntemler de seçilebilir. Eğitim materyallerinin geliştirilmesi aşamasında, pilot eğitimlerin eğitmenlerine eğitimin amaçları, süreci ve sorumlulukları hakkında bilgi vermek ve onları CyberAgent müfredatını etkin bir şekilde

öğretmeye hazırlamak için eğitim verilecektir. Pilot eğitim süreci, kullanılan eğitim yöntemlerinin etkinliğini izlemek ve gerektiğinde ayarlamalar yapmak için öğrenenlerden ve eğitmenlerden geri bildirim toplanmasını da içerir.

Modüller farklı öğretim formatlarında yapılacaktır:

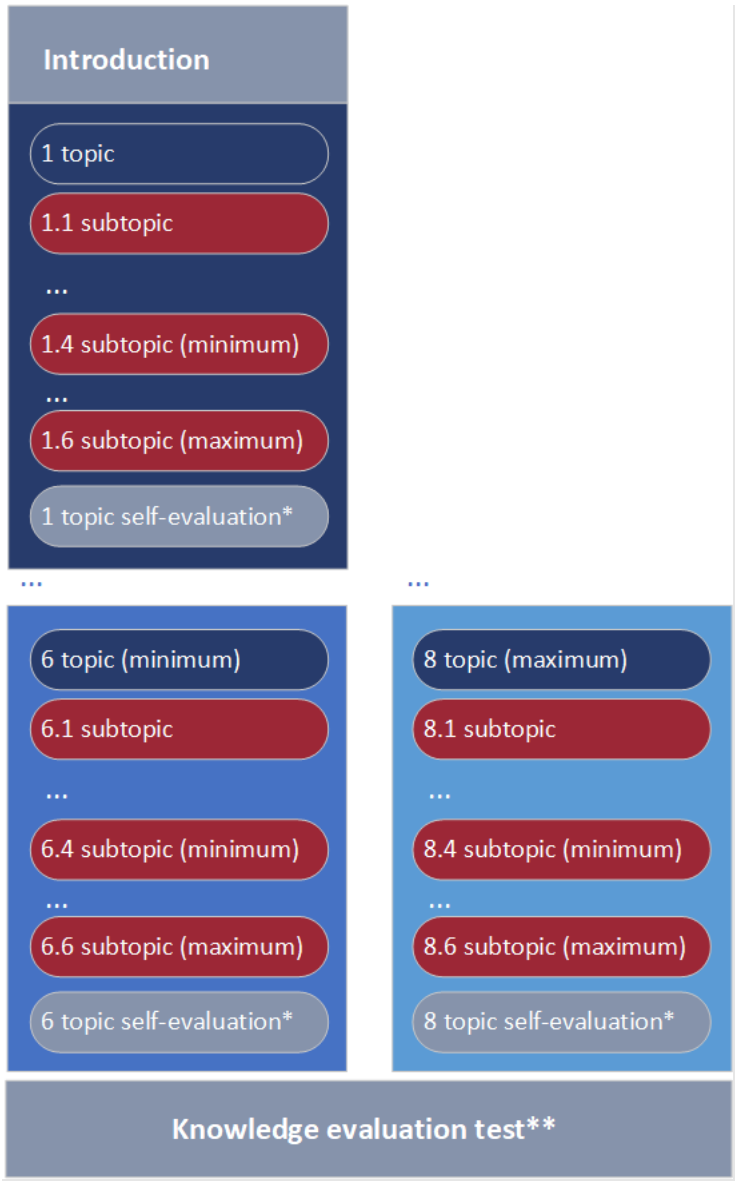
- uzak formatta**,**
- Senkron öğrenmede (öğretmenin tam desteği),
- asenkron **öğrenme** (gerektiğinde öğretmenin desteği), harmanlanmış öğrenme ve kendi kendine öğrenme.

Eğitimin farklı şekillerde verilmesi öngörüldüğünden, eğitim yöntemleri bu aşamada kılavuz olarak sunulmaktadır.

4. MODÜL YAPISI

VU Siber güvenlik çalışma programının modül yapısının analizi, uluslararası projelerin modül yapısının analizi (**Siber Kimlik Avı**, **SigortaIT**, **dComFra**) ve ticari platformların modül yapısının analizi, örneğin **Udemy (İngilizce)** ve **Kurs**, hem HEI hem de VET modüllerine uygulanabilecek tipik bir modül yapısının oluşturulmasına yol açmıştır.

Ana hedef, 8 modülün yükseköğretim öğrencileri (EQF seviye 5-6-), Mesleki Eğitim ve Öğretim öğrencileri ve KOBİ'ler (EQF seviye 4-5) ve her tür öğrenci için mikro modüller olmak üzere 8 modül geliştirmektir.



Şekil 11. Modül Yapısı

* Her bir alt konunun ardından self test (kendi kendine yansıtma) sorularının gelmesi önerilir. Bununla birlikte, modül geliştirme aşamasında, seçilen çalışmanın türüne bağlı olarak farklı bir

değerlendirme yöntemi veya seçeneği seçilebilir, örneğin öğrencilere pratik alıştırmalar, simülasyonlar vb. verilebilirken, bağımsız öğrencilere kendi kendine test soruları sunulur.

** Bilgi değerlendirme testi isteğe bağlıdır. Öğrenci, edindiği bilgiyi doğrulamak için bir kurs bitirme sertifikası almak isterse, bu test zorunludur. Ancak öğrenci, eğitime katıldığını kanıtlamak için kurs bitirme sertifikası alma seçeneğine sahiptir, bu durumda bu test isteğe bağlıdır.

Her eğitim modülünün pratik uygulanabilirlikle doğrudan bağlantılı olmasını sağlamak için, her modülün açıklaması, teorinin pratikte nasıl uygulandığına dair net örnekler sağlayacaktır. Bu, yalnızca modüllerin uygulanabilirliği için ayrıntılı senaryoları değil, aynı zamanda öğrencilerin teorik bilgileri gerçek siber güvenlik durumlarında pekiştirmek için üstlenecekleri belirli görevleri de içerir.

Her modül, farklı oranlarda Teknik beceriler, Analitik beceriler, Risk yönetimi becerileri, Organizasyon becerileri sağlamalıdır. Öz değerlendirme testi, modülün (konunun) herhangi bir bölümünün sonunda öğrencilerin bilgilerini test etmek için sağlanır. Bu sadece edinilen bilginin ölçülmesine veya değerlendirilmesine izin vermekle kalmaz, aynı zamanda öğrencinin ilerlemesi kaydedilir ve katılımcı, katılımcının öğrenme sürecine daha fazla dahil olmasını sağlayan puanlar ve rozetler toplar.

Her AKTS'nin 25-30 saatlik iş yükü olduğu AKTS formalitelerini takip etmek. Buna göre her modül 5 AKTS'ye eşit olabilir. İş yükü saatleri şu şekilde dağıtılabilir:

Masa 2. Saatlerce süren iş yükü

	Modül sayısı	**AKTS Toplamı**	**Teorik beceriler için uzak saatler**	**Pratik beceriler için uzak saatler**	**Bireysel çalışma saatleri**	**Toplam iş yükü saati**
Yükseköğretim öğrencileri için modüller (EQF seviye 5-6)	8	8-40	20%	20%	60%	200-1200
Mesleki Eğitim ve Öğretim Öğrencileri için Modüller (AYÇ seviye 4-5)	8	8-40	15%	25%	60%	200-1200
Bireysel çalışmalar (harmanlanmış öğrenme)	8	8-40	10%		90%	2000-1080
Bireysel çalışmalar (çevrimiçi)	8	8-40				200-1200
Mikro modüller	1-8	3-40				25-1200

Masa 3. Önerilen modüller iş yükü

Modül	Dersin AKTS Kredisi	Toplam saat	İletişim saatleri	İletişim saatleri (teori)	Temas saatleri (uygulama)	Bireysel çalışma saatleri
HEI Modülü başlığı	1-5	25-150	40%	20%	20%	60%
Mesleki Eğitim ve Öğretim Modülü başlığı	1-5	25-150	40%	15%	25%	60%
Bireysel çalışmalar (harmanlanmış öğrenme)	1-5	25-150	10%			90%
Bireysel çalışmalar (çevrimiçi)	1-5	25-150				100%
Mikro kesitler						10%-100%

Her modülün kendi açıklaması olmalıdır. Mikro kimlik bilgileri kullanılarak VU, Timtal ve diğer programların analizinden sonra, her bir CyberAgent modülü için tipik bir modül yapısı önerilmiştir (tipik bir modül yapısı örneği Ek 1'de verilmiştir).

Masa 4. CyberAgent modülleri için tipik yapı

Kategori	Detaylı bilgi
Modül tanımlama (modül hakkında temel bilgiler)	- Modül başlığı - Modül kodu - Öğretim görevlisi - Modülün teslim edildiği kurum veya departman - Teslimat modeli - Dil - Önkoşullar
Modül süresi ve iş yükü (açıkça zaman taahhüdü ve yapı taslağı)	- Toplam süre (AKTS sayısı) - Saatler içinde öğrenci iş yükü - Çalışma saatleriyle iletişime geçin - Bireysel çalışma saatleri

Eğitim hedefleri ve öğrenme çıktıları (modülün neyi başarmayı amaçladığı ve öğrencilerin ne öğreneceği hakkında ayrıntılar)	- Modülün amacı ve sonuçları
	- Dersin öğrenme çıktıları
	  o Teknik beceriler
	  o Analitik beceriler
	  o Risk becerileri
	  o Organizasyon becerileri

Öğretme ve Öğrenme Yöntemleri	- Öğretme ve öğrenme yöntemleri
Ölçme ve Değerlendirme (öğrencilerin nasıl değerlendirileceğine ilişkin açıklama)	- Değerlendirme yöntemleri - Görevler (laboratuvarlar, projeler, sunumlar, raporlar vb.) - Değerlendirme stratejisi, değerlendirme kriterleri
Kaynakları kolaylaştırın	- Ekipman, Yazılım ve Teknoloji
Kurs içeriği	- Modül konuları ve alt konuları
Kaynaklar	- Kaynakların listesi - Ek kaynaklar

Her AKTS 25-30 saat olarak kabul edilir (iletişim veya çevrimiçi saatler + bireysel çalışma).

Modül en az iki düzeyli bir hiyerarşiye sahip olmalıdır:

- **Hiyerarşinin ilk seviyesi** – konular. Bu seviyede, modülün ana unsurları giriş, giriş testi, final testi ve temel unsur - konu olabilir.
- **Hiyerarşinin ikinci seviyesi** – alt konular, modülün ana eğitim unsurları.

Hiyerarşinin ilk düzeyindeki her modül şunları içermelidir:

- **Modüle GİRİŞ** (metinsel açıklama, video tanıtımı): modülün uygunluğu ve faydaları, modülün temel amaçları ve çıktıları, gerekli yazılım ve donanım, katılımcılar için gereksinimler.
- **KONULAR** – dersin ana konuları, teorik materyal ve teorik öğretim yöntemleri.
- **ALT KONU** – Her konunun alt konusu, pratik, analitik analiz ve görevler, pratik ve analitik öğretim yöntemleri. Konular ve alt konular, metinsel bilgiler, videolar, ses klipleri, sunumlar, daha fazla okuma için bağlantılar içerebilir.
- **MODÜL Giriş testi** (gerekirse). Orta ve ileri seviyelerdeki giriş testi, başvuru sahibinin önceki seviyelerde yeterli bilgi ve beceriye sahip olduğunu doğrulamalıdır.
- **MODÜL onay testleri**. Teşekkür testi, bir öğrencinin becerilerinin objektif olarak doğrulanmasını sağlamalı ve modül gereksinimlerine uygunluğunu göstermelidir.
- **Mentorlar / öğretmenler için KILAVUZLAR**. Bu belge, mentorlar / öğretmenler için modül eğitim öğelerinin kullanımına ilişkin metodolojik öneriler içermelidir.

Hiyerarşinin ikinci düzeyindeki her KONU şunları içermelidir:

- **GİRİŞ** Konunun amaçları ve çıktıları, kısa içerik.
- **ALT KONULAR:** Öğrencinin ilgili becerilerde ustalaşmasını desteklemek için gerekli tüm eğitim unsurları.
- **TOPIC testi**: Mentorlar / öğretmenler için modülün uygulanması ve uygulanması hakkında kısa öneriler. Her ALT KONU, içeriği modül açıklamasının görevlerine karşılık gelen eğitim öğelerinden oluşmalıdır. Her alt konu, öğrencinin ilgili becerilerde yeterince yüksek düzeyde ustalaştığını doğrulayan bir Alt Konu TESTİ içerebilir (içermelidir).

Modülün eğitim materyalleri, her birinde 4-6 alt konu ve en az bir konu testi bulunan 6-8 konunun çalışılmasını desteklemelidir. Bu nedenle, modül (yaklaşık) 30-40 eğitim öğesi (bölüm öğretim yöntemlerinde açıklanan yöntemler) ve 6-8 test ve bir modül final teşekkür testi içermelidir.

5. CYBERAGENT MÜFREDATI VE EĞITIM PROGRAMI

Müfredat oluşturma yol haritası

CyberAgent Müfredatı ve Eğitim Programı, ACM, IEEE, AIS SIGSEC ve IFIP'in (2017) ortak görev gücü tarafından geliştirilen Siber Güvenlikte Ortaöğretim Sonrası Derece Programları için

Müfredat Yönergelerini takip eder[8] (bundan böyle - **Yönergeler olarak anılacaktır**). Daha spesifik olarak, CyberAgent projesinin genel odak noktası, Avrupa KOBİ'lerinin kurum içi siber güvenlik yeterliliklerini artırmak olduğundan, müfredat, bu Kılavuzların önerileri olarak Organizasyonel Güvenlik bilgi alanı çerçevesini takip etmektedir.

Bununla birlikte, müfredat oluşturmanın ilk adımı, CyberAgent projesinde önceden tanımlanmış alt konuları ve modülleri, Yönergeler tarafından önerilen ve açıklanan bilgi birimleri ve temel konularla eşleştirmektir (s. 59-70). Haritalama, proje ortakları tarafından tartışıldığı ve kararlaştırıldığı gibi, bu iki sütun arasındaki mantıksal korelasyona dayanmaktadır.

İkinci adım, T2.2 "KOBİ Siber Güvenlik Değişim Ajanları için eğitim ihtiyaçlarının haritalanması"nda tanımlanan ve açıklanan belirli öğrenme çıktılarını, yukarıda haritalanan bilgi birimi ve temel konularla birlikte atamaktır. Burada, siber güvenlikle ilgili farklı mesleklerin, yukarıda belirtilen T2.2 çıktısında açıkça belirtildiği gibi, çeşitli farklı bilgi, beceri ve yeterliliklere sahip olabileceği belirtilecektir. Bununla birlikte, aşağıda verilen teklif, CyberAgent'ın belirli mesleklerin veya stajyer gruplarının özel ihtiyaçlarına göre uyarlanabilecek beklenen bilgi, beceri ve yeterlilikleri yansıtmaktadır.

Bununla birlikte, bu müfredat oluşturma alıştırmasının sonuçları aşağıdaki Tablo 5'te verilmiştir.

[8] Siber Güvenlik Eğitimi Ortak Görev Gücü. (2017). Siber Güvenlikte Ortaöğretim Sonrası Derece Programları için Müfredat Yönergeleri: Bilgisayar Müfredatı Serisinde Bir Rapor. Bilgisayar Makineleri Derneği, 31 Aralık 2017. Şuradan ulaşılabilir: **https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf** [Erişim tarihi: 3 Mart 2024]

Masa 5. Müfredat oluşturma yol haritası

Alt Konular ve Modüller	Bilgi Birimi ve Temel Konular	Dersin öğrenme çıktıları HEI	Mesleki Eğitim ve Öğretim Derslerinin öğrenme çıktıları
Teknik beceriler			
- **Siber güvenlik tehditleri ve ilgili yasal konular hakkında güncellenmiş bilgi**	**Güvenlik Programı Yönetimi** - Proje yönetimi - Kaynak yönetimi - Güvenlik ölçümleri - Kalite güvencesi ve kalite kontrol	**Bilgi**: Öğrenciler, karmaşık siber tehditler ve saldırı vektörleri, ulusal ve uluslararası siber güvenlik mevzuatı, standartları ve sektörleriyle ilgili uyumluluk gereksinimleri dahil olmak üzere gelişmiş siber güvenlik ilkeleri hakkında ileri düzeyde bilgi edineceklerdir. **Beceriler**: Öğrenciler, gelişmiş metodolojiler ve araçlar kullanarak belirlenen riskleri azaltmak için gelişmiş risk değerlendirme ve yönetim stratejileri tasarlama ve uygulama becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, kuruluşun hedefleri ve uyumluluk yükümlülükleriyle uyumlu stratejik siber güvenlik politikaları ve çerçeveleri uygulayan siber güvenlik projelerine ve ekiplerine liderlik etme ve yönetme konusunda yetkin olacaklardır.	**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. **Beceriler**: Öğrenciler, gelişen siber tehditlere karşı koruma için araçlar ve yazılımlar kullanma ve kuruluşlarındaki genel güvenlik ölçümlerini ve kalite kontrolünü geliştirmek için proje ve kaynak yönetiminde sağlam güvenlik uygulamaları uygulama becerisine sahip olacaklardır. **Yetkinlikler**: 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 bildirme konusunda yetkin olacaklardır.

- **Siber güvenlik tehditleriyle nasıl başa çıkılacağına dair pratik bilgiler**	**Sistem Yönetimi** - İşletim sistemi yönetimi - Veritabanı sistemi yönetimi - Ağ yönetimi - Bulut yönetimi - Siber-fiziksel sistem yönetimi - Sistem güçlendirme - Kullanılabilirlik	**Bilgi**: Öğrenciler, işletme, veritabanı, ağ, bulut ve siber-fiziksel sistem yönetimi ve diğer alanlarda ileri düzeyde bilgi edinecek ve en son siber güvenlik savunma mekanizmalarını uygularken sistemleri etkili bir şekilde sağlamlaştırmalarına ve kullanılabilirliği sağlamalarına olanak tanıyacaktır. **Beceriler**: Öğrenciler, işletim sistemleri, veritabanları, ağlar ve bulut altyapıları dahil olmak üzere güvenli sistem mimarileri tasarlamak ve uygulamak için gelişmiş metodolojileri ve araçları kullanma becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, sistem yönetimi için stratejik siber güvenlik çerçeveleri geliştirme ve uygulama, sistem güçlendirme ve kullanılabilirliğini artırmak için projelere ve ekiplere liderlik etme ve çeşitli idari alanlarda sağlam siber güvenlik uygulamalarını sürdürmede etik kararlar alma konusunda yetkin olacaklardır.	**Bilgi**: Öğrenciler, etkili risk yönetimi politikaları uygularken, kimlik avı, fidye yazılımı ve DDoS saldırıları gibi yaygın siber tehditlere karşı işletim sistemlerini, veritabanlarını, ağları, bulutları ve siber-fiziksel sistemleri nasıl yönetecekleri ve güvenli hale getirecekleri konusunda pratik bilgiler edineceklerdir. **Beceriler**: Öğrenciler, çeşitli sistem platformlarında potansiyel siber güvenlik risklerini ve güvenlik açıklarını belirleme, sistem güçlendirmeyi ve kullanılabilirliğini artırmak için özel araçlar ve yazılımlar kullanma ve güvenli parola oluşturma, güvenli tarama ve hassas verilerin güvenli kullanımı gibi temel siber güvenlik uygulamalarını uygulama becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, sistem yönetimi içindeki güvenlik tehditlerini değerlendirme ve azaltma, siber güvenlik sorunlarını etkili bir şekilde iletme ve herhangi bir tehdit ve ihlali uygun kurumsal kanallara derhal bildirme konusunda yetkin olacaklardır.

Analitik beceriler			
- **Eleştirel düşünme zihniyeti**	**Analitik Araçlar** - Performans ölçümleri (metrikler) - Veri analizi - Güvenlik istihbaratı	**Bilgi**: Öğrenciler, ulusal ve uluslararası siber güvenlik mevzuatı, standartları ve uyumluluk gereksinimleri ve kendi sektörleriyle ilgili diğerleri hakkında ileri düzeyde bilgi sahibi olacaklardır. **Beceriler**: Öğrenciler, etkili risk yönetimi stratejileri tasarlamak ve uygulamak için performans ölçümlerini, veri analitiğini ve güvenlik istihbaratını kullanma becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, eleştirel düşünme zihniyetiyle stratejik siber güvenlik politikaları geliştirmek için analitik araçları kullanma konusunda yetkin olacak ve siber güvenlik uygulamalarında kurumsal hedefler ve uyumluluk yükümlülükleriyle uyumlu kararlar alacaklardır.	**Bilgi**: Öğrenciler, kurumsal varlıkları korumak için performans ölçümlerinin, veri analitiğinin ve güvenlik istihbaratının nasıl uygulanacağı konusunda pratik bilgiler edineceklerdir. **Beceriler**: Öğrenciler, potansiyel siber güvenlik risklerini ve güvenlik açıklarını belirlemek, siber güvenlik uygulamalarını güçlendirmek için veriye dayalı içgörüler uygulamak ve parolaların, taramanın, e-postanın ve veri işlemenin güvenliğini değerlendirmek ve geliştirmek için performans ölçümlerini kullanmak için analitik araçları kullanma becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, analitik araçları kullanarak potansiyel güvenlik tehditlerini değerlendirme ve azaltma, tehditleri ve ihlalleri kuruluşlarındaki uygun kanallara doğru bir şekilde bildirme konusunda yetkin olacaklardır.
- **Yerel tehditleri, nasıl meydana geldiklerini, risk altındaki kişileri vb. analiz edin ve anlayın.**	**Güvenlik Operasyonları** - Güvenlik birleşimi - Küresel güvenlik operasyon merkezleri (GSOC'ler)	**Bilgi**: Öğrenciler, küresel güvenlik operasyon merkezlerinden elde edilen içgörüleri ve siber güvenlik savunma stratejilerindeki mevcut eğilimleri kullanarak yerel siber tehditler	**Bilgi**: Öğrenciler, yerel siber tehditler ve kökenleri hakkında pratik bilgi edinecek, bu tehditlerin kurumsal varlıkları nasıl etkilediğini değerlendirecektir. **Beceriler**: Öğrenciler, güvenli parola oluşturma, güvenli tarama ve kendi özel

		hakkında ileri düzeyde bilgi edineceklerdir. **Beceriler**: Öğrenciler, etkili risk yönetimi stratejileri tasarlamak ve yerel siber güvenlik tehditlerini etkili bir şekilde azaltmak için planlar geliştirmek için küresel güvenlik operasyonları merkezlerinde gelişmiş metodolojileri ve araçları kullanma becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, küresel güvenlik operasyon merkezlerini kullanarak yerel tehditleri ele alan stratejik siber güvenlik politikaları geliştirme ve uygulama konusunda yetkin olacaklardır.	ortamlarına göre uyarlanmış güvenli veri işleme gibi araçları ve yazılımları kullanarak yerel siber güvenlik risklerini ve güvenlik açıklarını belirleme becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, küresel güvenlik operasyon merkezlerinden gelen içgörüleri kullanarak yerel güvenlik tehditlerini değerlendirme ve azaltma, siber güvenlik sorunlarını etkili bir şekilde iletme ve tehditleri ve ihlalleri kuruluşlarındaki uygun kanallara doğru bir şekilde bildirme konusunda yetkin olacaklardır.
Risk yönetimi			
- **KOBİ işyerine siber güvenlik rutinleri sağlamayı ve tanımlamayı öğrenin**	**Risk Yönetimi** - Risk tanımlama - Risk değerlendirmesi ve analizi - İçeriden gelen tehditler - Risk ölçme ve değerlendirme modelleri ve metodolojileri - Risk kontrolü	**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 tanıyacaklardır. **Beceriler**: Öğrenciler, kapsamlı risk değerlendirmeleri yapmak, etkili risk	**Bilgi**: Öğrenciler, KOBİ işyerlerini etkin bir şekilde korumak için risk tanımlama, değerlendirme ve kontrol süreçleri ve risk yönetimi stratejileri hakkında pratik bilgiler edineceklerdir. **Beceriler**: Öğrenciler, KOBİ ortamlarındaki potansiyel siber güvenlik risklerini belirleme ve analiz etme, tehdit azaltma için uygun araçları ve yazılımları kullanma ve güvenli parola oluşturma, güvenli tarama ve hassas verilerin güvenli bir

		yönetimi stratejileri tasarlamak ve uygulamak ve KOBİ işyerleri için özel olarak uyarlanmış sağlam siber güvenlik rutinleri geliştirmek için gelişmiş metodolojiler ve araçlar uygulama becerisine sahip olacaklardır. **Yeterlilikler**: Öğrenciler, KOBİ işyerleri için stratejik siber güvenlik politikaları geliştirme ve uygulama konusunda yetkin olacaklardır.	şekilde işlenmesi dahil olmak üzere temel siber güvenlik uygulamalarını teşvik etme ve uygulama konusunda yetenekli olacaklardır. **Yetkinlikler**: Öğrenciler, KOBİ işyerlerindeki güvenlik tehditlerini değerlendirme ve azaltma, siber güvenlik sorunlarını ve prosedürlerini etkili bir şekilde iletme ve ilgili tehditleri ve ihlalleri uygun kurumsal kanallara doğru bir şekilde bildirme konusunda yetkin olacaklardır.
- **Siber güvenlik için kendi işyeri KOBİ el kitabını oluşturun ve nasıl takip edileceğini öğrenin**	**İş Sürekliliği, Felaket Kurtarma ve Olay Yönetimi ve Personel Güvenliği** - Olay müdahalesi - Olağanüstü durum kurtarma - İş sürekliliği - Güvenlik farkındalığı, eğitim ve öğretim - Güvenlik işe alma uygulamaları - Güvenlik sonlandırma uygulamaları - Üçüncü taraf güvenliği - Gözden geçirme süreçlerinde güvenlik	**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. **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	**Bilgi**: Öğrenciler, olay müdahalesi, felaket kurtarma, iş sürekliliği ve personel güvenliği, kurumsal varlıkları ve hassas verileri koruma stratejilerini içeren kapsamlı bir KOBİ işyeri siber güvenlik el kitabının nasıl oluşturulacağı konusunda pratik bilgiler edineceklerdir. **Beceriler**: Öğrenciler, potansiyel siber güvenlik risklerini belirleme, tehditlere karşı koruma sağlamak için araçlar ve yazılımlar kullanma ve güvenli parola oluşturma, göz atma, e-posta güvenliği ve veri korumasını ele alan bir KOBİ el kitabı geliştirmek ve sürdürmek için siber güvenlikte en iyi uygulamaları uygulama becerisine sahip olacaklardır.

	- Çalışan kişisel bilgilerinin gizliliğine ilişkin özel sayı	siber güvenlik el kitabı oluşturma ve sürdürme becerisine sahip olacaklardır. **Yetkinlikler**: Öğrenciler, KOBİ'ler için bir siber güvenlik el kitabı geliştirme ve uygulama, güvenlik projelerine ve ekiplerine etkin bir şekilde liderlik etme, kurumsal hedeflere ve uyumluluk yükümlülüklerine uyum sağlama konusunda yetkin olacaklardır.	**Yetkinlikler**: Öğrenciler, özelleştirilmiş siber güvenlik el kitaplarında belirtildiği gibi, güvenlik tehditlerini değerlendirme ve azaltma, siber güvenlik politikalarını ve uygulamalarını etkili bir şekilde iletme ve KOBİ'lerindeki güvenlik olaylarını sistematik olarak bildirme konusunda yetkin olacaklardır.
Organizasyon becerileri			
- **KOBİ işyerlerinde siber güvenlik alanında yeni rutinlerin ve çalışma şeklinin nasıl uygulanacağı**	**Güvenlik Yönetişimi ve Politikası** - Organizasyonel bağlam - Gizlilik - Yasalar, etik ve uyumluluk - Güvenlik idaresi - Yönetici ve yönetim kurulu düzeyinde iletişim - Yönetim politikası	**Bilgi**: Öğrenciler, mevcut siber güvenlik ilkelerini, eğilimlerini 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. **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. **Yetkinlikler**: Öğrenciler, stratejik siber güvenlik politikaları geliştirme ve	**Bilgi**: Öğrenciler, siber güvenlik mevzuatına, bilgi güvenliği, risk yönetimi ve veri koruma politikalarına uygun olarak yeni siber güvenlik rutinlerini ve uygulamalarını KOBİ işyerlerine nasıl entegre edecekleri konusunda pratik bilgiler edineceklerdir. **Beceriler**: Öğrenciler, yeni güvenlik rutinleri uygulamak, riskleri belirlemek ve azaltmak ve KOBİ işyerlerinin yönetişim çerçevesinde güvenli parola oluşturma, tarama ve veri işleme gibi temel siber güvenlik uygulamalarını teşvik etmek için siber güvenlik araçlarını ve yazılımlarını uygulama konusunda yetenekli olacaklardır. **Yetkinlikler**: Öğrenciler, potansiyel güvenlik tehditlerini değerlendirme ve

		uygulama, KOBİ işyerlerinde yeni rutinler ve iş akışları oluşturmaya yönelik girişimlere liderlik etme ve kurumsal hedefler ve uyumluluk gereksinimleriyle uyumlu etik kararlar alma konusunda yetkin olacaklardır.	azaltma, siber güvenlik değişikliklerini ve politikalarını etkin bir şekilde iletme ve KOBİ'lerdeki güvenlik olaylarını yönetişim ve uyumluluk gereksinimlerine göre doğru bir şekilde raporlama konusunda yetkin olacaklardır.
- **Siber güvenlik alanında lider desteği vermek.**	**Siber Güvenlik Planlaması** - Stratejik planlama - Operasyonel ve taktiksel yönetim	**Bilgi**: Öğrenciler, gelişmiş siber güvenlik ilkelerini ve mevcut eğilimleri stratejik planlama ve operasyonel yönetime nasıl entegre edecekleri konusunda ileri düzeyde bilgi edineceklerdir. **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 yetenekli olacaklardır. **Yetkinlikler**: Öğrenciler, stratejik siber güvenlik çerçeveleri geliştirme ve uygulama, siber güvenlik girişimlerini yönetme ve yönetme konusunda yetkin olacaklardır.	**Bilgi**: Öğrenciler, kurumsal varlıkları korumak, ilgili mevzuat ve standartlara uymak ve etkili bilgi güvenliği stratejileri ve risk yönetimi politikaları uygulamak için stratejik planlama ve operasyonel yönetimin siber güvenliğe nasıl entegre edileceği konusunda pratik bilgiler edineceklerdir. **Beceriler**: Öğrenciler, siber güvenlik risklerini belirleme, tehditlere karşı koruma sağlamak için stratejik planlama ve operasyonel yönetim araçlarını kullanma ve liderlik destek rollerinde temel siber güvenlik uygulamalarının uygulanmasını teşvik etme konusunda yetenekli olacaklardır. **Yetkinlikler**: Öğrenciler, güvenlik tehditlerini değerlendirme ve azaltma, siber güvenlik stratejilerini ve sorunlarını etkili bir şekilde iletme ve olayları ve güvenlik açıklarını kuruluşlarındaki uygun kanallara güvenilir bir şekilde bildirme konusunda yetkin olacaklardır.

6. DERS DEĞERLENDIRME STRATEJISI

Bilginin değerlendirilmesi, öğrenme sürecinin ayrılmaz bir parçasıdır ve daha derin öğrenmeyi teşvik eder. Bu bölüm, CyberAgent kurslarındaki tüm katılımcıların gerekli öğrenme çıktılarını ve yeterliliklerini elde etmelerini sağlamak için gerekli olan kurs değerlendirme yaklaşımını açıklamaktadır. Kurstaki değerlendirme süreci iki ana bölüme ayrılmıştır: hem Yüksek Öğrenim (HEI) hem de Mesleki Eğitim ve Öğretim (VET) öğrencilerine farklı ihtiyaçları ve öğrenme hedefleri dikkate alınarak uyarlanmış öz değerlendirme ve bilgi değerlendirme testleri.

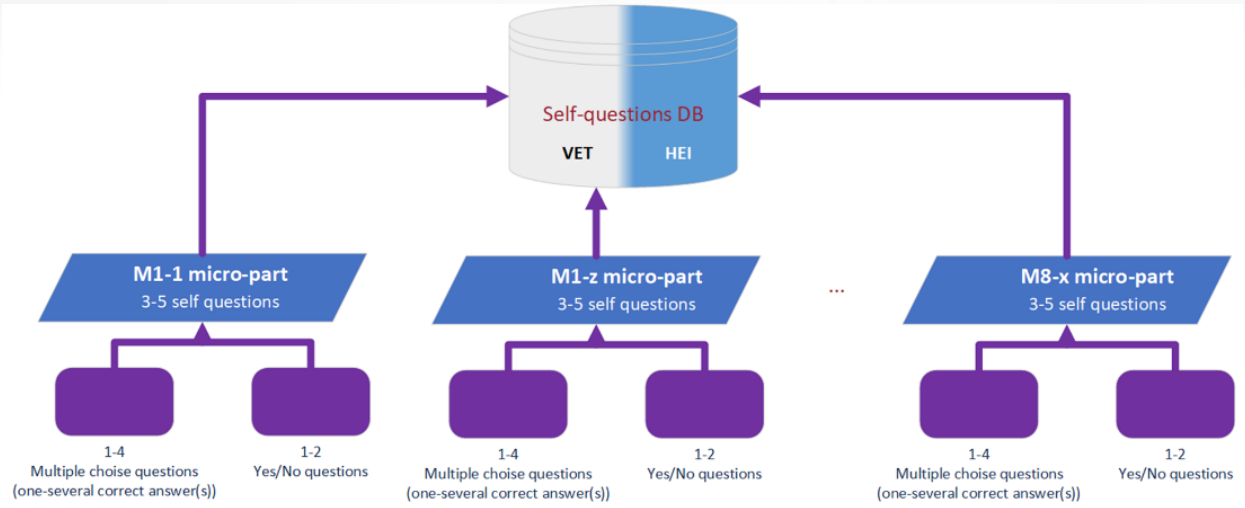
Modüllerin konuları hem HEI'ler hem de MEÖ için aynı olabileceğinden, bazı sorular hem HEI hem de MEÖ kursları için uygun olabilir. Böylece, soruları tasarlarken, sorunun yalnızca Mesleki Eğitim ve Öğretim veya HEI'ler için mi yoksa her ikisi için mi tasarlandığını belirtmek mümkün olacaktır. Bu işaretleme yöntemi, soruların tasarımını kolaylaştıracağı için yalnızca sorular tasarlanırken kullanılacaktır. Sorular platforma aktarıldıktan sonra, veritabanları Mesleki Eğitim ve Öğretim için farklı olacaktır.

Şekil 12. Öz değerlendirme ve bilgi değerlendirme veri tabanları

1. Öz değerlendirme testleri: Kurstaki her konunun tamamlanmasından sonra, öğrenciler öz değerlendirme testlerine tabi tutulacaktır. Bu değerlendirmeler, anında geri bildirim sağlamak için tasarlanmıştır ve öğrencilerin yakın zamanda kapsanan materyal hakkındaki anlayışlarını ölçmelerine yardımcı olur. Bu aşama, kendini yansıtmayı teşvik eder ve her konunun öğrenme hedeflerini pekiştirmeye yardımcı olur. Ek olarak, öğrencilerin daha fazla çalışmaya veya açıklamaya ihtiyaç duyabilecekleri alanları belirlemelerine olanak tanıyarak öğrenme yolculuklarına proaktif bir yaklaşımı teşvik eder.

Kurs katılımcıları, öz değerlendirme testlerini kullanarak başlangıçtaki bilgi düzeylerini belirleyebilir ve her eğitim konusundan sonra ilerlemeyi kontrol edebilir.

Doğru/yanlış, eşleştirme ve/veya çoktan seçmeli soruların karışımını içeren 3-5 soruluk bir öz değerlendirme sınavı önerilir. Başka bir konu ancak tüm sorular doğru cevaplandıktan sonra açılmalıdır. Denemelerde herhangi bir zaman sınırı veya kısıtlama olmamalıdır. Deneme, ilgili veri tabanından rastgele sorular seçmelidir.



Şekil 13. Öz değerlendirme veri tabanı yapısı

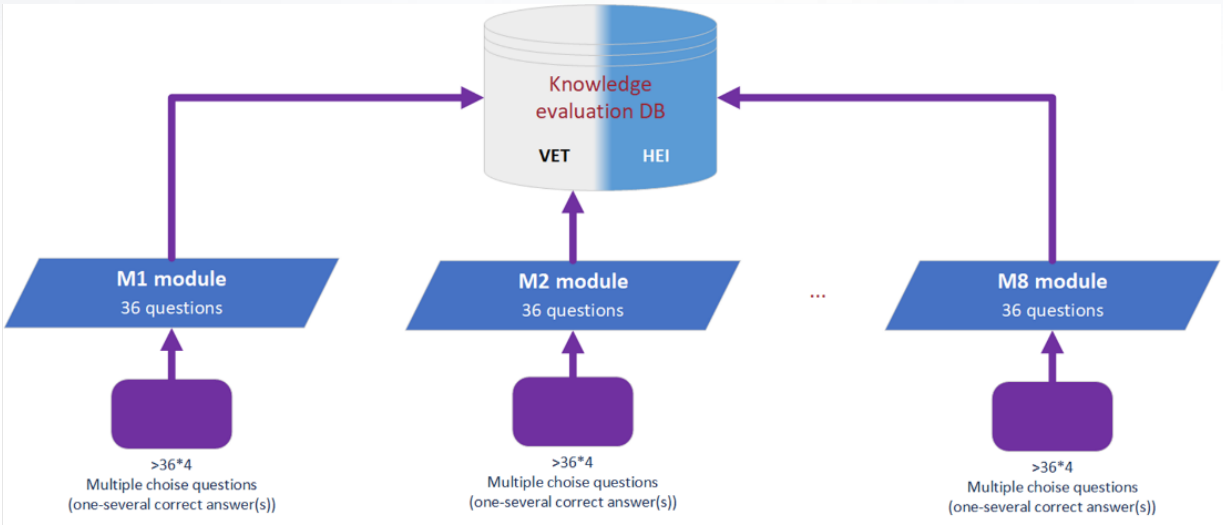
2. Bilgi değerlendirme testi*: Kurstaki tüm konuları tamamladıktan sonra, öğrencilerin kurs bitirme sertifikası alabilmeleri için bir final sınavına girmeleri gerekecektir. Bu kapsamlı değerlendirme, kurs içeriğine ilişkin genel anlayışlarını ve ustalıklarını değerlendirir. Son test, öğrencilerin materyali akılda tutmalarını değerlendirir ve bilgilerini daha geniş bir bağlamda ne kadar iyi uygulayabileceklerini belirler.

* Müfredat ve materyallerin geliştirilmesi sırasında, katılımcıların analitik ve eleştirel düşünme becerilerinin daha kapsamlı bir şekilde değerlendirilmesine olanak sağlayacak vaka çalışmaları, pratik alıştırmalar ve yansıtıcı raporlar gibi kursun tamamlanmasını ve bilginin değerlendirilmesini değerlendirmek için diğer metodolojiler dikkate alınacaktır. Bu yaklaşım, ders sunumunda HEI ve MEÖ öğrencileri için öğretim görevlilerine de sunulacaktır.

Kurs katılımcıları, bilgi değerlendirme testini kullanarak nihai bilgi seviyelerini belirleyebilir ve başarılı olmaları halinde bir kurs tamamlama rozeti (sertifika) alabilirler.

Doğru/yanlış, eşleştirme ve çoktan seçmeli soruların karışımını içeren 36 soruluk bir bilgi değerlendirme testi önerilir. 45 dakikalık bir zaman sınırı olmalı ve yalnızca tek denemeye izin verilmelidir. Test, bir veri tabanından rastgele sorular seçilerek uygulanmalıdır.

Ek olarak, değerlendirme aynı zamanda hile önlemeyi de dikkate almalı ve bu nedenle yaklaşık dört soru seti geliştirilmelidir. Hem Mesleki Eğitim ve Öğretim hem de Mesleki Eğitim (HEI) için bazı bilgi testi soruları çakışabilir, bu nedenle geliştirme sırasında üç özniteliğimiz olacaktır: Mesleki Eğitim ve Öğretim, HEI veya VET ve HEI.



Şekil 14. Bilgi değerlendirme veri tabanı yapısı

Bu iki aşamalı değerlendirme stratejisi, yalnızca çoklu geri bildirim döngüleri sağlayarak etkili öğrenmeyi desteklemekle kalmaz, aynı zamanda öğrencilerin eğitimlerinde aktif rol almalarını sağlar.

Öz değerlendirme testleri ve bilgi değerlendirme testleri, derslerin müfredatına uygun olarak ve bu projede geliştirilen sonuçlar ve öneriler temelinde geliştirilecektir.

SORU VERITABANI KOMPOZISYONU

Yeterince geniş ve dengeli bir soru tabanı sağlamak için, Mesleki Eğitim veya Öğretim kursundaki her konu için en az 5 doğru/yanlış veya eşleşen soru ve 5 çoktan seçmeli soru oluşturulacaktır.

Her derste en az 10 konu olacağını varsayarsak, her bir Mesleki Eğitim veya Öğretim kursunun genel temeli en az %10-20 doğru/yanlış veya eşleştirme ve %90-80 çoktan seçmeli sorular içermelidir. Bu genel bir kılavuzdur, ancak öğretmen dersin konusuna göre soruların yapısını seçme olanağına sahip olacaktır.

Mesleki Eğitim ve Öğretim öğrenme hedefleri ve sonuçlarındaki farklılıklar göz önüne alındığında, tek bir ders için soru veri tabanının genel bileşimi aşağıdaki tabloda gösterildiği gibi içermelidir.

Masa 6. Soru türleri

	Doğru/yanlış veya eşleşen sorular	**Çoktan seçmeli sorular**
Kursun genel kısmı	20%	80%
Kursun Mesleki Eğitim ve Öğretime özel kısmı	20%	80%
Kursun HEI'ye özel kısmı	20%	80%

Mesleki Eğitim ve Öğretim kursları için toplam:	20%	80%

SORU OLUŞTURMA YÖNERGELERI

Öz değerlendirme ve bilgi değerlendirme testleri için sorular İngilizce olarak hazırlanmalı ve daha sonra ortak dillere yerelleştirilmelidir.

Kurs içinde hem öz değerlendirme hem de bilgi değerlendirmesi için test soruları geliştirirken, soruların açık, özlü ve geçmişlerine bakılmaksızın tüm adaylar için erişilebilir olmasını sağlamak esastır. Bu yaklaşım, değerlendirmelerin öğrencilerin ders içeriğini anlamalarını ve ders müfredatında belirtilen beceri ve hedeflere ulaşma becerilerini doğru bir şekilde yansıtmasını sağlar.

Soru oluşturma için genel yönergeler:

Test sorularının geliştirilmesinde açık yönergeler uygulanacaktır: sorular, karmaşık terminoloji veya kafa karıştırıcı ifadeler kullanılmadan anlaşılır ve kursun öğrenme hedefleriyle doğrudan ilişkili olmalıdır. Tüm kurs katılımcıları için adalet ve erişilebilirlik sağlamak için kültürel olarak spesifik veya kafa karıştırıcı sorulardan da kaçınılacaktır. Soruların tasarımı hakkında daha fazla rehberlik aşağıda verilmiştir.

Açıklık ve basitlik: Sorular basit olmalı, adayların kafasını karıştırabilecek veya yanıltabilecek karmaşık dil veya jargon kullanımından kaçınmalıdır. Amaç, adayların karmaşık soruları deşifre etme yeteneklerini değil, konuyla ilgili bilgi ve anlayışlarını değerlendirmektir.

Doğrudanlık ve uygunluk: Her soru doğrudan ders müfredatının temel becerileri ve hedefleriyle ilgili olmalıdır. Amaçlanan öğrenme çıktılarını değerlendirmeye odaklanmayı sürdürmek için alakasız veya teğetsel içerikten kaçınılmalıdır.

Kültürel ve arka plan duyarlılığı: Soruların belirli kültürel bilgi veya deneyimleri varsaymadığından emin olun, bu da onları farklı geçmişlere sahip adaylar için erişilebilir ve adil hale getirir.

Zor sorular yok: Adayları yanıltma veya kandırma girişiminde bulunmadan, her sorunun amacı açık olmalıdır. Adayları yakalamak veya hileleri tespit etme yeteneklerini test etmek için tasarlanmış sorular, konuyu anlamalarını etkili bir şekilde değerlendirmez.

Açık ve özlü sunum: Sorular, tüm adayların soruyu aynı şekilde anlamasını sağlayacak şekilde yoruma yer bırakmayacak şekilde ifade edilmelidir. Soruları kısa tutun, ana noktayı gizleyebilecek gereksiz uzunluklardan kaçının.

Olumlu ifadeler: Sorularda olumsuz ifadeler kullanmaktan kaçının (örneğin, "Aşağıdakilerden hangisi DEĞİLDİR..."). Olumsuz ifadeler, özellikle sınav koşullarında kafa karışıklığına ve yanlış

yorumlamaya yol açabilir. Bunun yerine, netliği artırmak için tüm soruları olumlu bir şekilde çerçeveleyin.

Soru yapımı için özel yönergeler:

Çoktan seçmeli sorular: Tüm seçeneklerin makul ve soruyla alakalı olduğundan emin olun. Doğru cevap tartışmasız bir şekilde doğru olmalı, çeldiriciler ise materyali anlayan biri için açıkça yanlış olmalıdır.

Doğru/Yanlış soruları: Kurs içeriğiyle doğrudan ilgili olan açık ve gerçeklere dayalı ifadeler sunarak doğruluk değerleri konusunda herhangi bir belirsizlik olmamasını sağlayın.

Eşleştirme soruları: Her iki listenin de (ör. bir taraftaki terimler ve diğer taraftaki tanımlar) açıkça ilişkili olduğundan ve her eşleştirmeyi yapmak için basit bir temel olduğundan emin olun. Bazı öğelerin kullanılmayacağı veya birden çok kez kullanılabileceği açıkça belirtilmedikçe, öğe sayısının aynı hizada olmadığı eşit olmayan listelerden kaçının.

Pilot eğitim, hem öğrencilerden hem de eğitmenlerden geri bildirim toplayarak bilgi değerlendirme metodolojileri ve değerlendirme süreci hakkındaki bilgileri analiz edecektir. Bu, bilgi değerlendirme yöntemlerinin uygunluğunun değerlendirilmesine ve gerekirse değerlendirme yaklaşımının tamamlanmasına veya iyileştirilmesine izin verecektir.

OYUNLAŞTIRMA

Bu bölüm, CyberAgent kurslarında uygulanan oyunlaştırma öğelerinin açıklamasını tanıtır. Oyunlaştırma, katılımcıların motivasyonunu ve katılımını artırmak için oyunlaştırma ilkelerini geleneksel öğrenme etkinliklerine dahil etme sürecidir. Bu unsurlar, oyunlaştırmanın öğrenme performansını önemli ölçüde artırabileceğini, öğrencilerin öğrenme motivasyonunu artırabileceğini ve öğrenme sürecine katılımlarını artırabileceğini gösteren eğitim teknolojisi üzerine yapılan en son araştırmalara dayanarak seçilmiştir.

Kurslara entegre edilecek oyunlaştırma unsurları arasında katılımcının deneyim ve başarılarını yansıtan rozetler, puanlar, rütbeler ve renk kodlu takma adlar yer alıyor.

- Rozetler şunlar için verilecektir:

- **Modülün tamamlanması**.
- **Geçme yüzdesine göre bir testi geçmek için**. Örneğin, bir katılımcıya final sınavında minimum geçme puanı için bronz rozet, minimum %75 geçme puanı için gümüş rozet, %76-%90 geçme puanı için altın rozet ve %90-%100 geçme puanı için platin rozet verilecektir. Bu durumda, bir katılımcının bu türden 8 rozeti olabilir.
- **Konu tamamlanıyor**.
- **On gün boyunca her gün sisteme giriş yapmak**.
- **Kurs danışmanı/eğitmeni tarafından her konu için** özel bir etkinlik rozeti de verilecektir.

- **Öz değerlendirme test puanları + çarpanlı final test puanları temelinde hesaplanan** puanlar ve puanlar.

CyberAgent kurs katılımcıları ilerlemelerini bireysel olarak göremeyecekler, ancak gruplar veya takımlar halinde diğer katılımcılarla rekabet edebilecekler (atılan en yüksek puana ve aynı zamanda en çok rozete göre). Bu, sadece bireysel değil, aynı zamanda işbirliği becerilerinin geliştirilmesinde önemli olan takım rekabetini ve işbirliğini de teşvik eder.

Her katılımcı, kursa giriş yaptığında, kursun ilerlemesine ve toplanan deneyime (tamamlanan / kaydedilen kurslar) göre renk kodlu olacak takma adını görecektir.

Bu, kurs katılımcılarının kendilerini eğitim sürecine daha iyi dahil etmelerine yardımcı olacaktır. Kurs katılımcıları, puanlarını yükseltmek için aynı testi birkaç kez tekrarlayabilir (puanlar, doğru şekilde yapılan en yüksek sayıda öz değerlendirme testi için verilir).

Özel bir algoritma, cevaplamak için geçen süreyi, testin tekrarlanma sayısını ve diğer parametreleri dikkate alarak her katılımcının puanını hesaplayacak ve böylece kopya çekme olasılığını en aza indirecektir.

Tüm oyunlaştırma kuralları net bir şekilde tanımlanacak ve katılımcılara iletilecek, böylece herkes farklı oyunlaştırma seviyelerine nasıl ulaşılabileceğini ve bunların nasıl hesaplandığını kolayca anlayabilecektir.

7. CYBERAGENT ÖĞRENME/ÖĞRETME SÜRECI

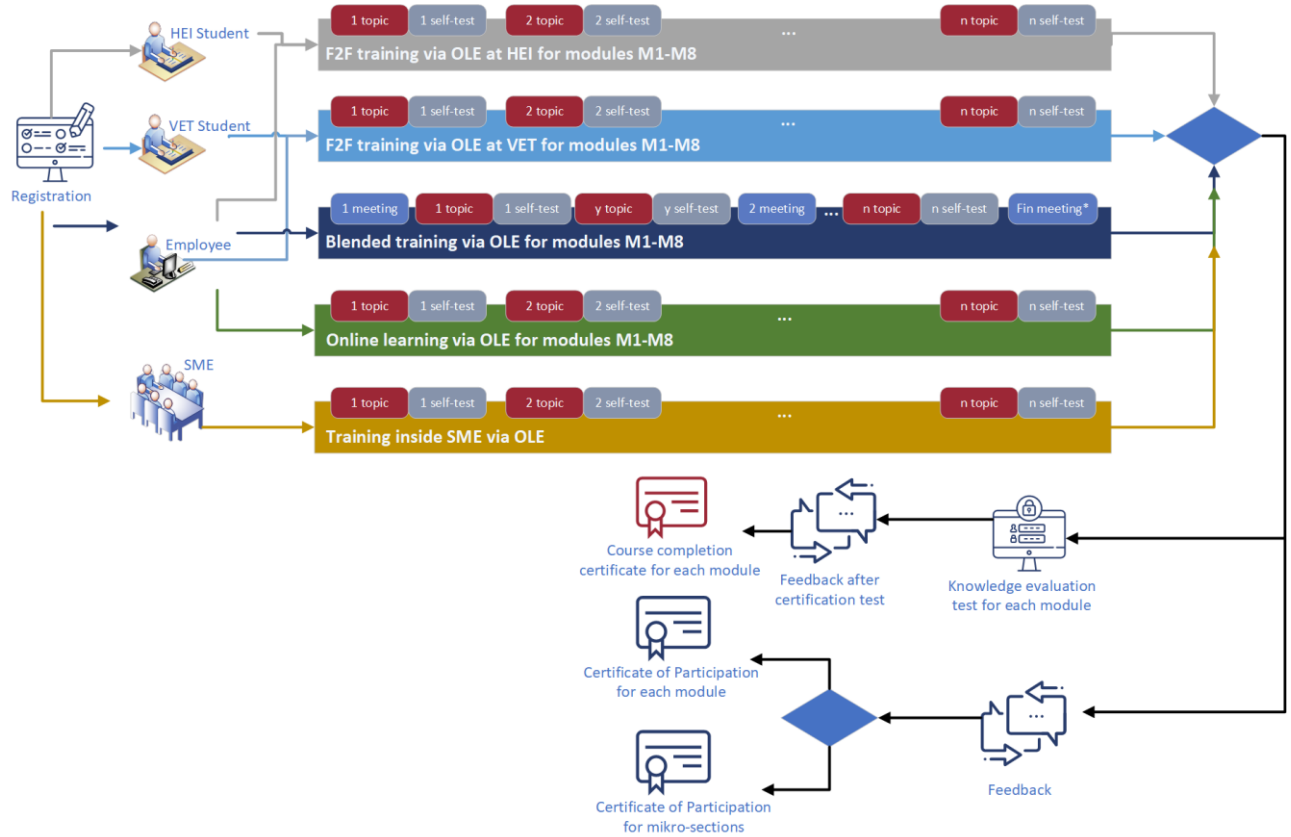
Bu bölüm, bu belgedeki tüm bölümlerdeki bilgileri özetlemekte ve öğrenme platformunda bir CyberAgent kursuna kaydolma ile başlayan ve kursun tamamlanması veya bir sertifikanın verilmesiyle sona eren öğrenme/öğretme sürecini ayrıntılı olarak açıklamaktadır.

CyberAgent kursları, Yüksek Öğretim Kurumlarından (HEI'ler), Mesleki Eğitim ve Öğretim (VET) öğrencileri ve KOBİ'lerden çalışanlar da dahil olmak üzere çok çeşitli öğrencilere hitap edecek şekilde tasarlanmıştır. Her katılımcıya, kişisel koşullarını ve eğitim kurumunun organizasyon politikalarını göz önünde bulundurarak kendilerine en uygun öğrenme yolunu seçme fırsatı vermeyi amaçlıyoruz.

Seçilen öğrenme/eğitim yöntemine rağmen katılımcılar CyberAgent platformuna kayıt olurlar ve eğitim süresince platformu kullanırlar.

Kayıt

CyberAgent kursuna kaydolmak isteyen aday katılımcılar, istedikleri modülleri ve tercih ettikleri öğrenme yöntemini seçerek bir kayıt formu doldurmalıdır. Katılımcılara birinci modülden sekizinci CyberAgent modülüne kadar olan öğrenme yolu boyunca rehberlik etmek için kavramsal bir diyagram sağlanmıştır.



Şekil 15. CyberAgent öğrenme / öğretme yolu

Katılımcıların bilgilerinin gizliliği, özellikle GDPR gereklilikleri ile ilgili olarak, kayıt işlemi sırasında sağlanacaktır. Kayıt sırasında katılımcılar, eğitim platformunun kuralları, gizlilik ve veri koruma kuralları hakkında bilgi edinme fırsatına sahip olacaklardır.

Katılımcı kayıt verilerine, kuruluşun iç politikalarına uygun olarak, yalnızca ortakların kuruluşundaki belirlenmiş kişiler erişebilir. Pilot eğitim oturumları sırasında, proje ortaklarından gelen katılımcı verilerine CyberAgent koordinatörü tarafından erişilebilir ve diğer ortakların birbirlerinin katılımcı verilerini görmelerine izin verilmez. Projenin tamamlanmasının ardından koordinatör, proje sonucunda belirtildiği gibi, proje sonuçlarından sonra 5 yıla kadar proje sonuçlarını izlemek için yalnızca diğer ortakların anonimleştirilmiş verilerine erişebilir.

Farklı hedef gruplarımızın ihtiyaçlarını karşılamak için özel eğitim seçenekleri sunuyoruz. HEI ve VET öğrencileri, üniversite iletişim oturumları aracılığıyla eğitime katılabilirler. KOBİ çalışanları, ihtiyaçlarına en uygun öğrenme yöntemini seçebilirler: harmanlanmış öğrenme, yalnızca çevrimiçi veya daha az yaygın olarak HEI veya VET derslerine katılmak.

Eğitim, birden fazla çalışanı olan daha büyük şirketlere de sunulabilir. Bu gibi durumlarda, eğitim yöntemi, CyberAgent modül kurslarını dahil etmeye devam ederken belirli ihtiyaçları karşılayacak şekilde özelleştirilecektir.

Platforma kaydolduktan sonra, katılımcılar öğrenme yöntemlerini seçer ve çalışmalarına başlarlar. Bir modülü veya bir modülün bir bölümünü tamamladıktan sonra, bir katılımcının modül testini en az %75 puanla geçmesi durumunda verilen bir Katılım Sertifikası veya Kurs Tamamlama Sertifikası almaya hak kazanabilirler.

Son olarak, katılımcıların herhangi bir sertifika almadan önce bir geri bildirim formu doldurmaları gerekmektedir. Bu geri bildirim, eğitim tekliflerimizin sürekli iyileştirilmesi ve katılımcı memnuniyetinin sağlanması için çok önemlidir.

Öğrenme/eğitim yolları

Çalışanların kurs içeriğiyle etkileşim kurmak için çeşitli seçenekleri vardır:

- Yükseköğretim kurumları veya Mesleki Eğitim kurumları çalışanların misafir katılımcı olarak katılmasına izin veriyorsa, çalışan kayıtlı öğrencilerle birlikte derslere katılabilir. Bu tür dış katılımcı oturumları, yayınlanan ders programına göre yılda 1-2 kez düzenlenebilir.
- Çalışanlar, eğitim oturumlarının önerilen 2-4 ay süreyle belirli tarihlerde yürütüldüğü karma bir eğitim yaklaşımını tercih edebilir. Grup başına en fazla 30 katılımcı olmak üzere en az 10 katılımcıdan oluşan gruplar tavsiye edilir. Harmanlanmış eğitim, doğrudan geri bildirimi ve nihai değerlendirmeye hazırlanmayı kolaylaştırmak için kursun başında, sırasında ve sonunda hem yüz yüze hem de çevrimiçi istişareleri içerir.
- Çalışanlar, kursun tamamlanması için belirli bir süre olmaksızın, kendi hızınızda öğrenme için çevrimiçi öğrenme yolunu seçebilirler.
- CyberAgent modülleri hakkında daha fazla ayrıntı Bölüm 1'de verilmiştir. Çalışma yolu.

Öğrenci katılımı

Siber güvenlik çalışma programına kayıtlı öğrenciler, akademik kurumlarının düzenlemelerine bağlı olarak farklı yollarla karşılaşabilirler. CyberAgent modüllerinin bir kısmını veya tamamını tamamlamaları gerekebilir veya dahili üniversite politikalarına bağlı olarak, kriterleri karşılayan öğrenciler bir veya daha fazla CyberAgent modülünü incelemeyi seçebilirler. HEI veya VET öğrencileri, genellikle kurumları tarafından sağlanan geleneksel sınıf eğitimi yoluyla konularla ilgilenir veya nihai bilgi değerlendirme testine hazırlanmak için kendi kendine çalışma yöntemlerini tercih edebilir.

KOBİ katılımı

Siber güvenlik eğitiminin gerekli görüldüğü kuruluşlarda, şirketten bir temsilci kuruluşu şirket içi eğitim oturumları için kaydedebilir. Bu gibi durumlarda, üniversite ve/veya eğitmenler ile ayrı bir anlaşma yapılarak, eğitim yöntemi, program ve sertifikaların verilmesi, mevcut modüllere dayalı olarak kuruluşun özel ihtiyaçlarına göre uyarlanabilir.

Geri Bildirim Toplama

Modül tamamlandıktan sonra, katılımcıların çevrimiçi olarak erişilebilen anonim bir geri bildirim formu doldurmaları gerekmektedir. Geri bildirim verilerine yalnızca iş ortağının kuruluşundaki yetkili personel erişebilir ve pilot eğitim oturumları ve proje sonrası veri kullanımı sırasında benzer gizlilik önlemleri uygulanır.

Geri bildirim esas olarak kurs katılımcılarından toplanacaktır, ancak mentorlardan/eğitmenlerden de geri bildirim alınacaktır. Toplanan geri bildirimler, katılımcıların organizasyonel memnuniyet düzeyini, kurs organizasyonunun yönlerini, öğrenme sürecini, edinilen yeterliliklerin pratikte kullanımını, kursun içeriğini, değerlendirme stratejilerini, oyunlaştırma öğelerinin dahil edilmesini, iyileştirme alanlarını vb. değerlendirecektir.

Geri bildirimlerin sonuçları, hızlı tepki vermek ve eğitim stratejilerini gerçek ihtiyaçlara ve pazar değişikliklerine göre geliştirmek için düzenli olarak gözden geçirilecek ve proje yönetim ekibine sunulacaktır.

Katılımcılar ancak bu formu doldurduktan sonra katılım sertifikası veya kurs bitirme sertifikası veya katılım sertifikası almaya hak kazanırlar.

Kurs Bitirme Sertifikası

Değerlendirme testinin başarıyla tamamlanması, katılımcı için bir kurs bitirme sertifikasının oluşturulmasıyla sonuçlanır. Modül başına bir son test vardır.

Katılım sertifikası

Bilgi değerlendirme sınavına girmemeyi tercih eden katılımcılara katılım sertifikası verilebilir. Bu onay, kurs içindeki tek bir modülün veya birkaç mikro parçanın tamamlanmasının ardından verilebilir.

SONUÇLAR VE ÖZET

Bu rapor, KOBİ siber güvenlik değişim temsilcileri için, yükseköğretim kurumundan Mesleki Eğitim ve Öğretime ve doğrudan KOBİ çalışan eğitimine kadar çeşitli eğitim ve profesyonel düzeylerdeki özel ihtiyaçları ele almak üzere uyarlanmış yapılandırılmış öğrenme yollarını başarıyla geliştirmiştir. Sekiz kapsamlı modülden oluşan müfredat, geleceğin siber güvenlik uzmanlarının etkili bir şekilde güçlendirilmesi için çok önemli olan teknik, analitik, organizasyonel ve risk yönetimi becerilerini bütünleştirir.

Öğrenme yollarına yönelik yapılandırılmış yaklaşım, KOBİ çalışanları için kapsamlı bir eğitim yolculuğu sağlar. Öğrenme Öncesi, Öğrenme ve Öğrenme Sonrası aşamaları aracılığıyla bilginin kalıcılığını ve pratik uygulamayı destekler. Mikro modüller, bireysel ihtiyaçlara esneklik ve uyarlanabilirlik sunarak, tanınmış nitelikler sağlayan mikro kimlik bilgileriyle öğrenmeyi geliştirir. Endüstri standartlarıyla bu uyum, KOBİ'lerdeki siber güvenlik yeteneklerinin güçlendirilmesine önemli ölçüde katkıda bulunur ve çalışanları mevcut zorluklarla ve gelecekteki gelişmelerle başa çıkmaya hazırlar. Aşağıdaki Carrier Pathway analizi, ESCO çerçevesi tarafından tanımlanan siber güvenlik rollerinin ilerlemesini haritalandırarak, bireyleri siber güvenlik iş gücüne etkili bir şekilde entegrasyona hazırlayan ve nihayetinde kariyer beklentilerini ve mesleki gelişimlerini geliştiren hedefli bir eğitim yaklaşımını kolaylaştırmıştır.

Siber güvenlik müfredatındaki pedagojik yaklaşımların araştırılan çeşitliliği, farklı öğrenme stillerini ve ihtiyaçlarını barındıran dinamik ve esnek bir öğrenme ortamına izin vermelidir. Teorik dersler, pratik laboratuvarlar, oyunlaştırma ve işbirlikçi projeler dahil olmak üzere çeşitli öğretim yöntemlerinin dahil edilmesi, öğrencilerin yalnızca bilgi alıcıları değil, aynı zamanda öğrenme yolculuklarında aktif katılımcılar olmalarını sağlar. Bu kapsamlı strateji, katılımı, anlayışı geliştirmeli ve öğrencileri gerçek dünyadaki siber güvenlik zorluklarına daha iyi hazırlamalıdır. Öğretim yöntemlerinin modüle özgü gereksinimlere uyarlanabilirliği, öğrenme deneyimini daha da kişiselleştirmeli ve her öğrenci için eğitim sonuçlarının en üst düzeye çıkarılmasını sağlamalıdır.

Müfredat, CyberAgent projesinin alt konularını ve modüllerini uluslararası kabul görmüş bilgi birimleriyle sistematik olarak eşleştirerek, siber güvenlik alanının dinamik gereksinimlerini karşılamakla kalmaz, aynı zamanda öngörür. Bu metodik yaklaşım, her bir öğrenme kazanımının, siber güvenlik tehditlerinin etkili yönetimi için çok önemli olan gerçek dünya yetkinlikleriyle stratejik olarak bağlantılı olmasını sağlar. Müfredatın uyarlanabilirliği, sektördeki çeşitli profesyonel rollere hizmet etmesine olanak tanıyarak, öğrencileri yalnızca acil zorluklara değil, aynı zamanda siber güvenlikte uzun vadeli kariyer gelişimine de hazırlar.

Ana hatlarıyla belirtilen kurs değerlendirme stratejisi, öğrencilerin siber güvenlik programlarındaki yeterliliklerini ve ilerlemelerini değerlendirmek için bir çerçeve sunar. Öz değerlendirme testlerini ve kapsamlı bilgi değerlendirme testlerini birleştiren iki aşamalı yaklaşım, öğrencilerin materyalle aktif olarak ilgilenmelerine, anlayışlarını sürekli olarak değerlendirmelerine ve öğrenme stratejilerini buna göre ayarlamalarına olanak tanır. Strateji, değerlendirmeyi hem yükseköğretim kurumlarını hem de Mesleki Eğitim ve Öğretim

öğrencilerini özel sorularla barındıracak şekilde tasarlayarak, her eğitim seviyesi için uygunluk ve uygunluk sağlayarak öğrenme deneyimini geliştirir. Bu yöntem, öğrencinin ustalığının ve bilgilerini pratik olarak uygulamaya hazır olduğunun net bir ölçüsünü sağlar. Ayrıca, rozetler ve puanlama sistemleri gibi oyunlaştırma öğelerinin tanıtılması yalnızca öğrencileri motive etmekle kalmaz, aynı zamanda rekabetçi ancak işbirlikçi bir öğrenme ortamını da teşvik eder.

Son olarak, CyberAgent öğrenme ve öğretme süreci, yükseköğretim kurumlarından, Mesleki Eğitim kurumlarından ve KOBİ'lerden çok çeşitli öğrenciler için uygun kapsamlı ve uyarlanabilir bir eğitim çerçevesi sağlar. Bu sistem, yüz yüze, karma ve çevrimiçi öğrenme dahil olmak üzere çeşitli katılımcı yöntemlere izin vererek, siber güvenlik eğitiminin nasıl verildiği ve erişildiği konusunda esneklik sağlar. CyberAgent platformuna kayıt, katılımcıların tercih edilen modülleri ve öğrenme yöntemlerini seçtikleri ve başarılı bir şekilde tamamlandıktan ve değerlendirildikten sonra sertifikaların verilmesiyle sonuçlanan bir yol başlatır. Bu yapı yalnızca kişiselleştirilmiş öğrenme yörüngelerini desteklemekle kalmaz, aynı zamanda eğitim süreci boyunca katılımcı gizliliğini korumak için gerekli olan katı gizlilik standartlarıyla da uyumludur.

Bu belgede sağlanan öneriler ve rehberlik, CyberAgent'ın kapsamlı eğitim müfredatını, eğitim materyallerini, bilgi testlerini ve değerlendirmelerini, uygulama alıştırmalarını ve CyberAgent eğitim platformuna entegre edilecek diğer eğitim içeriğini geliştirmek için bir sonraki aşamada kullanılacaktır.

EK 1. MODÜL AÇIKLAMASI

MODÜL AÇIKLAMASI

Modül başlığı	Modül kodu
...	

Öğretim Görevlisi(ler)i	Modülün teslim edildiği kurum veya departman
...	...

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

Önkoşullar
...

Tahsis edilen AKTS kredisi sayısı	Öğrencinin iş yükü	Çalışma saatleriyle iletişime geçin	Bireysel çalışma saatleri
5	...	...	...

Modülün amacı ve sonuçları		
...		
Modülün öğrenme çıktıları	**Öğretme ve öğrenme yöntemleri**	**Değerlendirme yöntemleri**
Teknik beceriler		
Analitik beceriler		
Risk becerileri		
Organizasyon becerileri		

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

Modül içeriği: konuların dökümü	Çalışma saatleriyle iletişime geçin					Bireysel çalışma saatleri ve görevler	
	Dersler (HEI/VET)	Danışmanlıklar (KOBİ'ler)	Uygulama (HEI/VET)	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		…
HEI/VET sertifikası -> Kendi kendine test I + …+ Kendi kendine test n + Bilgi değerlendirme testi		
KOBİ'ler/Kendi kendine çalışmalar sertifikası -> Kendi kendine test I + …+ Kendi kendine test n + Bilgi değerlendirme testi		
Mikro modüller, mikro kesit -> Kendi kendine sınama I (isteğe bağlı), Kendi kendine sınama n (isteğe bağlı)		

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 okuma
…

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@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