T.C.
FIRAT ÜNİVERSİTESİ
TEKNİK BİLİMLER MESLEK YÜKSEKOKULU
SİBER GÜVENLİK ANALİSTLİĞİ VE OPERATÖRLÜĞÜ PROGRAMI
DERS MÜFREDATI

1. SINIF I. YARIYIL

DERS KODU	DERSİN ADI	Z/S	T	U	K	AKTS
SGP1101	Temel Programlama I	Z	2	2	3	5
SGP1103	Bilişim ve Ağ Teknolojisi Temelleri	Z	3	2	4	6
SGP1105	Matematik ve Mantık	Z	3	0	3	4
SGP1107	Siber Güvenliğe Giriş	Z	2	0	2	3
SGP1109	İşletim Sistemleri ve Güvenliği	Z	3	2	4	6
YDİ107	İngilizce I	Z	2	0	2	2
AİT101	Atatürk İlkeleri ve İnkılap Tarihi I	Z	2	0	2	2
TRD109	Türk Dili I	Z	2	0	2	2
Toplam			**19**	**6**	**22**	**30**

T: Teori U: Uygulama Z:Zorunlu S:Seçmeli AKTS: Avrupa Kredi Transfer Sistemi

1. SINIF II. YARIYIL

DERS KODU	DERSİN ADI	Z/S	T	U	K	AKTS
SGP1102	Temel Programlama II	Z	2	2	3	5
SGP1104	Güvenli Ağ Tasarımı ve Cihaz Yönetimi	Z	2	2	3	5
SGP1106	Siber Saldırılar ve Savunma Yöntemleri	Z	3	2	4	6
SGP1108	Güvenli Yazılım Geliştirme ve Yazılım Güvenliği	Z	3	2	4	6
SGP1110	İş Sağlığı ve Güvenliği	Z	2	0	2	2
YDİ108	İngilizce II	Z	2	0	2	2
AİT102	Atatürk İlkeleri ve İnkılap Tarihi II	Z	2	0	2	2
TRD110	Türk Dili II	Z	2	0	2	2
Toplam			**18**	**8**	**22**	**30**

T: Teori U: Uygulama Z:Zorunlu S:Seçmeli AKTS: Avrupa Kredi Transfer Sistemi

2. SINIF III. YARIYIL

DERS KODU	DERSİN ADI	Z/S	T	U	K	AKTS
SGP2101	Siber Olay Yönetimi I	Z	3	0	3	4
SGP2103	Mesleki Uygulama	Z	0	2	1	6
SGP2105	Proje Yönetimi Metodolojileri ve Etkili İletişim	Z	2	0	2	2
SSD1101	Sosyal Seçmeli Ders-I	S	2	0	2	3
	Alan Seçmeli Ders I	S	3	0	3	5
	Alan Seçmeli Ders I	S	3	0	3	5
	Alan Seçmeli Ders II	S	3	2	4	5
Toplam			**16**	**4**	**18**	**30**
Alan Seçmeli Dersler I						
SGP2107	Kriptolojinin temelleri	S	3	0	3	5
SGP2109	Adli Bilişim	S	3	0	3	5
SGP2111	Yapay Zekâ ve Siber Güvenlik	S	3	0	3	5
SGP2113	Siber Güvenlik Yönetişimi	S	3	0	3	5
Alan Seçmeli Dersler II						
SGP2115	Nesne Tabanlı Programlama	S	3	2	4	5
SGP2117	İnternet Programlama	S	3	2	4	5

T: Teori U: Uygulama Z:Zorunlu S:Seçmeli AKTS: Avrupa Kredi Transfer Sistemi
En az 18 AKTS Seçmeli Ders Alması Gerekmektedir.

2. SINIF IV. YARIYIL

DERS KODU	DERSİN ADI	Z/S	T	U	K	AKTS
SGP2102	Siber Olay Yönetimi II	Z	3	0	3	4
SGP2104	Sızma Testi	Z	3	2	4	5
SGP2106	Mesleki İngilizce	Z	2	0	2	2
SSD2102	Sosyal Seçmeli Ders-II	S	2	0	2	3
	Alan Seçmeli Ders III	S	3	0	3	4
	Alan Seçmeli Ders III	S	3	0	3	4
	Alan Seçmeli Ders IV	S	2	2	3	4
	Alan Seçmeli Ders IV	S	2	2	3	4
Toplam			**20**	**6**	**23**	**30**
Alan Seçmeli Dersler III						
SGP2108	Bilişim Hukuku	S	3	0	3	4
SGP2110	Veri Yapıları ve Algoritma	S	3	0	3	4
SGP2112	Bulut Teknolojileri	S	3	0	3	4
SGP2114	Yeni Nesil Teknolojiler	S	3	0	3	4
Alan Seçmeli Dersler IV						
SGP2116	Web ve Uygulama Güvenliği	S	2	2	3	4
SGP2118	Zararlı Yazılım Analizi ve Tespiti	S	2	2	3	4
SGP2120	Veri Tabanı Uygulamaları ve Güvenliği	S	2	2	3	4
SGP2122	Mobil Teknolojiler ve Güvenlik	S	2	2	3	4

T: Teori U: Uygulama Z:Zorunlu S:Seçmeli AKTS: Avrupa Kredi Transfer Sistemi
En az 19 AKTS Seçmeli Ders Alması Gerekmektedir.

1.SINIF I. YARIYIL

Ders Kodu	Ders Adı	Z/S	T	U	K	AKTS
AİT101	**Atatürk İlkeleri ve İnkılap Tarihi I**	**Z**	**2**	**0**	**2**	**2**
Atatürk ilkeleri ve İnkılap Tarihi dersini okumanın amacı ve inkılap kavramı. Osmanlı İmparatorluğunun yıkılışını ve Türk İnkılabını hazırlayan sebeplere toplu bakış. Osmanlı İmparatorluğunun parçalanması. Mondros Ateşkes Antlaşması, işgaller karşısında memleketin durumu ve Mustafa Kemal Paşa'nın Samsun'a çıkışı. Milli mücadele için ilk adım, kongreler yolu ile teşkilatlanma, Kuvayı Milliye ve Misak-ı Milli, Türkiye Büyük Millet Meclisi'nin açılması. Türkiye Büyük Millet Meclisi'nin İstiklal Savaşı'nın yönetimini ele alması. Sakarya Zaferine kadar milli mücadele, Sakarya Savası ve Büyük Taarruz, Mudanya'dan Lozan'a, eğitim ve kültür alanında, milli mücadele, sosyal ve iktisadi alanda milli mücadele.						
TRD109	**Türk Dili I**	**Z**	**2**	**0**	**2**	**2**
Teorik: Dil, dilin tanımı, dilin özellikleri, dil aileleri, Türk dilinin tarihi dönemleri, ses bilgisi (Fonetik), şekil bilgisi (Morfoloji), sözcük türleri, eylem çatıları, yazılı ve sözlü anlatım türleri. Uygulama: Dil bilgisi konuları ve yazılı anlatımla ilgili ders içi çalışmalar yapmak.						
YDİ107	**İngilizce I**	**Z**	**2**	**0**	**2**	**2**
- Verb BE: Statements and Questions. Countries and Nationalities. - Present Simple Tense: Statements . Verbs for Daily Routines. - Present Simple Questions. Free Time Activities. - Verb: Have / Has. Family Tree. - There is / There are. Places in a Town. - Present Continuous Tense – Rooms and Furniture. - Can / Can't. Months of the Year. - Present Simple Tense vs. Present Continuous Tense. Jobs						
SGP1101	**Temel Programlama I**	**Z**	**2**	**2**	**3**	**5**
Bu dersin amacı, öğrencilere algoritmik düşünme ve problem çözme becerisi kazandırmak ve Python programlama dili üzerinden temel programlama kavramlarını öğretmektir. Öğrencilerin bir problemi analiz edebilmesi, algoritmasını oluşturabilmesi ve bu algoritmayı temel programlama yapılarını kullanarak çalışan bir programa dönüştürebilmesi hedeflenmektedir. Ders İçeriği algoritma ve programlamaya giriş; problem çözme ve algoritmik düşünme; akış şemaları ve sözde kod; Python programlama ortamı; değişkenler, sabitler ve veri tipleri; operatörler ve ifadeler; temel giriş-çıkış işlemleri; karar yapıları; döngüler; fonksiyonlara giriş; parametreler ve dönüş değerleri; karakter dizileri; liste, demet, sözlük ve küme gibi temel Python veri yapıları; temel hata ve istisna yönetimi; dosya işlemlerine giriş; modüler programlamanın temel prensipleri ve temel programlama uygulamaları.						
SGP1103	**Bilişim ve Ağ Teknolojisi Temelleri**	**Z**	**3**	**2**	**4**	**6**
Bu dersin amacı, öğrencilere bilgisayar sistemleri, işletim sistemleri, bilgisayar ağları ve internet teknolojilerinin temel çalışma prensiplerini öğretmek ve siber güvenlik alanındaki ileri dersler için gerekli teknik altyapıyı kazandırmaktır. Öğrencilerin bilgisayar donanım ve yazılım bileşenlerini tanıyabilmesi, temel ağ mimarilerini ve protokollerini anlayabilmesi, IP adresleme ve temel ağ yapılandırmalarını gerçekleştirebilmesi, ağ trafiğinin temel işleyişini analiz edebilmesi ve bilişim altyapılarındaki temel güvenlik gereksinimlerini kavrayabilmesi hedeflenmektedir. Ders İçeriği bilgi ve iletişim teknolojilerinin temel kavramları; bilgisayar sistemlerinin temel yapısı; işlemci, bellek, depolama ve giriş-çıkış birimleri; donanım ve yazılım arasındaki ilişki; sistem ve uygulama yazılımları; işletim sistemlerinin temel görevleri ve Windows/Linux işletim sistemlerine giriş; sanallaştırma kavramına giriş; bilgisayar ağlarının temel kavramları; ağ türleri ve topolojileri; LAN, WAN ve kablosuz ağlar; istemci-sunucu ve eşler arası ağ mimarileri; OSI ve TCP/IP katmanlı ağ modelleri; Ethernet ve temel veri bağlantı teknolojileri; MAC adresleme; IPv4 ve IPv6 adresleme; alt ağlara ayırma (subnetting) temelleri; TCP ve UDP protokolleri; port ve soket kavramları; anahtarlama (switching) ve yönlendirme (routing) prensipleri; switch, router, access point ve temel ağ cihazları; ARP, ICMP, DHCP, DNS ve temel internet protokolleri; NAT kavramı; HTTP/HTTPS ve temel uygulama katmanı protokollerine giriş; internetin temel yapısı ve çalışma prensipleri; kablolu ve kablosuz ağ teknolojileri; temel ağ yapılandırma ve sorun giderme yöntemleri; ping, traceroute, ipconfig/ifconfig/ip ve nslookup gibi temel ağ araçları; paket ve ağ trafiği kavramı; temel paket analizi ve Wireshark kullanımına giriş; ağ performansı, bant genişliği, gecikme ve paket kaybı kavramları; ağlarda temel güvenlik kavramları; güvenlik duvarı, ağ segmentasyonu ve güvenli iletişim kavramlarına giriş; temel ağ tehditlerine genel bakış; örnek bilgisayar ve ağ yapılandırmalarının uygulamalı olarak gerçekleştirilmesi.						

SGP1105	**Matematik ve Mantık**	**Z**	**3**	**0**	**3**	**4**
Bu dersin amacı, öğrencilere bilgisayar bilimleri ve siber güvenlik alanlarında ihtiyaç duyulan temel matematiksel düşünme, mantıksal akıl yürütme ve problem çözme becerilerini kazandırmaktır. Öğrencilerin mantıksal ifadeleri analiz edebilmesi, temel ayrık matematik yapılarını kullanabilmesi, algoritmik ve kriptografik problemlerin matematiksel altyapısını kavrayabilmesi ve siber güvenlik problemlerini matematiksel modeller üzerinden temel düzeyde değerlendirebilmesi hedeflenmektedir. Ders İçeriği matematiksel ve mantıksal düşünmenin temel kavramları; önermeler ve önerme mantığı; doğruluk tabloları; mantıksal bağlaçlar; mantıksal eşdeğerlikler; niceleyiciler ve yüklem mantığına giriş; çıkarım kuralları; temel ispat yöntemleri; doğrudan ispat, karşıt ters ve çelişki ile ispat; kümeler ve küme işlemleri; Kartezyen çarpım; bağıntılar ve özellikleri; eşdeğerlik bağıntıları; fonksiyonlar ve fonksiyon türleri; Boole cebiri ve mantıksal işlemler; ikili sayı sistemi ve farklı sayı sistemlerinin temel özellikleri; bölünebilme, asal sayılar, EBOB ve Öklid algoritmasına giriş; modüler aritmetik ve siber güvenlikteki temel kullanım alanları; kombinatorik ve temel sayma prensipleri; permütasyon ve kombinasyon; temel olasılık kavramları ve koşullu olasılığa giriş; çizge (graph) teorisinin temel kavramları; düğüm, kenar, yol, çevrim ve bağlılık; ağaç yapılarına giriş; çizgelerin bilgisayar ağları ve siber güvenlik problemlerindeki temel uygulamaları; matematiksel mantık, ayrık matematik ve olasılık kavramlarının programlama, algoritmalar, kriptografi ve siber güvenlik problemleriyle ilişkilendirilmesi.					
SGP1107	**Siber Güvenliğe Giriş**	**Z**	**2**	**0**	**2**	**3**
Bu dersin amacı, öğrencilere siber güvenliğin temel kavramlarını, prensiplerini, tehditlerini ve savunma yaklaşımlarını tanıtarak programın ilerleyen dönemlerinde alacakları mesleki dersler için kavramsal bir altyapı oluşturmaktır. Öğrencilerin bilgi varlıklarının korunmasına ilişkin temel güvenlik gereksinimlerini anlayabilmesi; tehdit, zafiyet, risk ve güvenlik kontrolü kavramları arasındaki ilişkileri kurabilmesi; temel siber saldırı ve savunma yaklaşımlarını tanıyabilmesi ve siber güvenliğin teknik, yönetsel, hukuki ve etik boyutları konusunda temel farkındalık kazanması hedeflenmektedir. Ders İçeriği siber güvenliğin temel kavramları ve gelişimi; siber uzay ve siber güvenlik ekosistemi; bilgi güvenliği ve siber güvenlik arasındaki ilişki; bilgi varlığı kavramı; gizlilik (Confidentiality), bütünlük (Integrity) ve erişilebilirlik (Availability) prensipleri; kimlik doğrulama, yetkilendirme ve hesap verebilirlik kavramları; tehdit, zafiyet, risk ve güvenlik kontrolü kavramları; saldırı yüzeyi ve temel tehdit modelleme yaklaşımı; siber tehdit aktörleri, motivasyonları ve hedefleri; siber saldırıların temel türleri ve saldırı yaşam döngüsüne giriş; zararlı yazılım, phishing, sosyal mühendislik, parola ve kimlik bilgilerine yönelik saldırılar, ağ ve web tabanlı saldırılara genel bakış; temel kriptografi kavramları ve kriptografinin siber güvenlikteki rolü; kullanıcı, parola ve çok faktörlü kimlik doğrulama güvenliği; işletim sistemi, ağ, yazılım, web uygulaması, veri ve uç nokta güvenliğinin temel kavramları; güvenlik duvarı, IDS/IPS, antivirüs/EDR ve diğer temel güvenlik kontrollerine giriş; erişim kontrolü ve en az ayrıcalık prensibi; katmanlı savunma (Defense in Depth) yaklaşımı; Zero Trust güvenlik yaklaşımına giriş; güvenlik logları, izleme ve siber olay kavramı; siber olay tespiti ve müdahale süreçlerine genel bakış; risk yönetimi, güvenlik politikaları ve siber güvenlik yönetişimine giriş; kişisel verilerin korunması ve mahremiyet konusunda temel farkındalık; siber güvenliğin hukuki ve etik boyutları; insan faktörü ve siber güvenlik farkındalığı; bulut bilişim, IoT, yapay zekâ ve gelişmekte olan teknolojilerin oluşturduğu temel siber güvenlik risklerine genel bakış; siber güvenlik meslekleri, SOC ve siber güvenlik analistinin temel görev ve sorumlulukları; güncel siber güvenlik olaylarının temel kavramlar çerçevesinde incelenmesi.					
SGP1109	**İşletim Sistemleri ve Güvenliği**	**Z**	**3**	**2**	**4**	**6**
Bu dersin amacı, öğrencilere modern işletim sistemlerinin temel çalışma prensiplerini öğretmek ve Windows ile Linux işletim sistemlerinin güvenli yapılandırılması, yönetilmesi, izlenmesi ve korunmasına yönelik temel bilgi ve uygulama becerileri kazandırmaktır. Ders kapsamında öğrencilerin işletim sistemi seviyesindeki güvenlik tehditlerini tanıyabilmesi, kullanıcı ve erişim yetkilerini yönetebilmesi, sistem kayıtlarını inceleyebilmesi, temel sistem sıkılaştırma işlemlerini gerçekleştirebilmesi ve uç nokta güvenliği mekanizmalarını kullanabilmesi hedeflenmektedir. Ders İçeriği işletim sistemlerinin temel yapısı ve çalışma prensipleri; Windows ve Linux işletim sistemleri; süreç, servis ve kaynak yönetimi; dosya sistemleri ve dosya erişim izinleri; kullanıcı, grup, rol ve ayrıcalık yönetimi; kimlik doğrulama ve yetkilendirme mekanizmaları; Linux ve Windows komut satırı yönetimi; Bash ve PowerShell'e giriş; sistem ve servislerin güvenli yapılandırılması; işletim sistemi sıkılaştırma (hardening) prensipleri; güvenlik güncellemeleri, yama ve zafiyet yönetimi; Windows Event Logs, Linux syslog/journald ve sistem kayıtlarının incelenmesi; audit ve güvenlik izleme mekanizmaları; süreç, servis ve ağ bağlantılarının güvenlik açısından analizi; Active Directory ve merkezi kimlik yönetimine giriş; uç nokta güvenliği, antivirüs ve EDR (Endpoint Detection and Response) kavramları; sanallaştırma ve konteyner güvenliğine giriş; temel işletim sistemi saldırı teknikleri, ayrıcalık yükseltme ve bunlara karşı koruma yöntemleri; Windows ve Linux sistemleri üzerinde uygulamalı güvenli yapılandırma ve olay analizi.					

1.SINIF II. YARIYIL

Ders Kodu	Ders Adı	Z/S	T	U	K	AKTS
AİT102	**Atatürk İlkeleri ve İnkılap Tarihi II**	**Z**	**2**	**0**	**2**	**2**
Büyük Millet Meclisinin Açılması ve Büyük Millet Meclisine Karşı İsyan Hareketleri. Kuvayı Milliye'den Düzenli Orduya Geçiş, Kurtuluş Savaşı'nda Cepheler, Barış ve Diplomasi Dönemi, Mudanya Ateşkes Antlaşması, Lozan Barış Antlaşması. Türk İnkılabının Genel Özellikleri, Siyasal Alanda Yapılan İnkılap Hareketleri, Hukuk, Eğitim ve Sosyal Alandaki inkılaplar. Atatürk Dönemi Türk Dış Politikası 1932-1938 (Milletler Cemiyeti, Balkan Antantı, Montreux Sözleşmesi, Sadabat Paktı, Hatay Sorunu). Atatürk İlkeleri (Cumhuriyetçilik, Milliyetçilik, Halkçılık, Devletçilik, Laiklik, İnkılapçılık)						
TRD110	**Türk Dili II**	**Z**	**2**	**0**	**2**	**2**
Teorik: Cümle bilgisi, kipler, anlatım bozuklukları, söz grupları, sözlü kompozisyon türleri ve güzel konuşma ile ilgili bilgileri öğrencilere kazandırmak. **Uygulama:** Cümle bilgisi ve sözlü anlatımla ilgili ders içi uygulamaları yapmak.						
YDİ108	**İngilizce II**	**Z**	**2**	**0**	**2**	**2**
- Past Simple: Verb BE. Evens and Places to Go - Past Simple Actions. School Subjects. - Past Simple Questions. Parts of the Body.- Future Tense : Be + Going to. Travel. - Countable and Uncountable Nouns. Food. - Adjectives. Clothes. - Comparatives Adjectives. Weather. - Superlatives Adjectives. Geographical Features.						
SGP1102	**Temel Programlama II**	**Z**	**2**	**2**	**3**	**5**
Bu dersin amacı, öğrencilerin Temel Programlama I dersinde kazandıkları programlama ve algoritmik problem çözme becerilerini ileri düzeye taşımaktır. Öğrencilerin Python programlama dilini kullanarak daha kapsamlı problemleri çözebilmesi, verileri etkin biçimde işleyebilmesi, programları modüler yapılar halinde tasarlayabilmesi ve temel algoritmik yaklaşımları uygulayabilmesi hedeflenmektedir. Ders İçeriği ileri Python programlama teknikleri; fonksiyonların ileri kullanımı; kapsam ve yaşam süresi; özyinelemeli (recursive) fonksiyonlar; lambda ifadeleri; yineleyiciler (iterators) ve üreteçler (generators); kapsamlı liste ve sözlük ifadeleri (comprehensions); temel veri yapılarının ileri kullanımı; arama ve sıralama algoritmalarına giriş; algoritma verimliliği ve temel karmaşıklık kavramları; dosya ve dizin işlemleri; metin ve yapılandırılmış veri işleme; CSV ve JSON verileriyle çalışma; hata ve istisna yönetimi; modül ve paket geliştirme; standart ve harici Python kütüphanelerinin kullanımı; hata ayıklama (debugging), test ve kod doğrulama; modüler program tasarımı ve ileri programlama uygulamaları.						
SGP1104	**Güvenli Ağ Tasarımı ve Cihaz Yönetimi**	**Z**	**2**	**2**	**3**	**5**
Bu dersin amacı, öğrencilere bilgisayar ağlarının güvenli biçimde tasarlanması, yapılandırılması, yönetilmesi ve izlenmesine yönelik temel bilgi ve uygulama becerileri kazandırmaktır. Öğrencilerin ağ cihazlarını güvenli biçimde yapılandırabilmesi, ağ trafiğini ve temel güvenlik olaylarını analiz edebilmesi, ağ segmentasyonu ve erişim kontrolü uygulayabilmesi ve güncel ağ güvenliği teknolojilerini temel düzeyde kullanabilmesi hedeflenmektedir. Ders İçeriği TCP/IP protokol ailesi ve ağ iletişiminin güvenlik açısından incelenmesi; IPv4 ve IPv6 adresleme; router, switch ve temel ağ cihazlarının yapısı ve güvenli yönetimi; LAN, WAN ve VLAN teknolojileri; ağ segmentasyonu ve mikro segmentasyon kavramlarına giriş; yönlendirme ve anahtarlama güvenliği; erişim kontrol listeleri (ACL); güvenlik duvarlarının yapısı, türleri ve güvenlik politikalarının oluşturulması; IDS/IPS sistemlerine giriş; NAT ve güvenli uzaktan erişim; VPN teknolojileri; kablolu ve kablosuz ağ güvenliği; DNS, DHCP ve temel ağ servislerinin güvenliği; ağ erişim kontrolü (NAC); Zero Trust ve Zero Trust Network Access (ZTNA) yaklaşımlarına giriş; ağ trafiğinin izlenmesi ve temel paket analizi; ağ logları, trafik kayıtları ve NetFlow kavramları; ağ güvenliği açısından temel telemetri ve izleme; SDN ve bulut ağ güvenliğine giriş; SASE/SSE kavramlarına genel bakış; ağ cihazlarında güvenli yapılandırma, güncelleme, yedekleme ve konfigürasyon yönetimi; güvenli ağ mimarisi oluşturma ve örnek ağ güvenliği senaryolarının uygulamalı olarak incelenmesi.						
SGP1106	**Siber Saldırılar ve Savunma Yöntemleri**	**Z**	**3**	**2**	**4**	**6**
Bu dersin amacı, öğrencilere güncel siber tehditleri, tehdit aktörlerini ve yaygın saldırı yöntemlerini öğretmek; saldırıların farklı aşamalarını analiz edebilme ve bu saldırılara karşı uygulanabilecek temel savunma mekanizmalarını değerlendirebilme becerisi kazandırmaktır. Öğrencilerin ağ, sistem, uygulama, kimlik ve kullanıcıları hedef alan saldırıları anlayabilmesi, saldırganların taktik, teknik ve prosedürlerini temel düzeyde değerlendirebilmesi ve katmanlı savunma yaklaşımı çerçevesinde uygun koruma, tespit ve müdahale yöntemlerini ilişkilendirebilmesi hedeflenmektedir. Ders İçeriği siber tehdit, zafiyet, risk ve saldırı kavramları; siber tehdit ortamı ve güncel tehdit eğilimleri; tehdit aktörleri, motivasyonları ve hedefleri; siber saldırı yaşam döngüsü ve saldırı yüzeyi kavramı; saldırgan taktik, teknik ve prosedürleri (TTP); MITRE ATT&CK çerçevesine giriş; keşif ve bilgi toplama; ilk erişim yöntemleri; phishing, spear phishing ve sosyal mühendislik saldırıları; parola ve kimlik bilgilerine yönelik saldırılar; credential theft ve credential abuse kavramları; zararlı yazılımlar, botnetler ve ransomware saldırıları; dosyasız (fileless) saldırılar ve Living-off-the-Land (LotL) yaklaşımına						

giriş; ağ tabanlı saldırılar; spoofing, Man-in-the-Middle, DoS/DDoS ve temel protokol saldırıları; kablosuz ağlara yönelik temel saldırılar; işletim sistemi ve servis zafiyetlerinin istismarı; ayrıcalık yükseltme ve kalıcılık kavramları; web ve uygulamalara yönelik temel saldırılar; veri ihlali ve veri sızdırma (data exfiltration) kavramları; bulut ve IoT ortamlarına yönelik temel tehditler; saldırı göstergeleri (Indicator of Compromise – IoC) ve temel saldırı davranışlarının belirlenmesi; güvenlik duvarları, IDS/IPS ve uç nokta güvenliği mekanizmaları; erişim kontrolü ve çok faktörlü kimlik doğrulama; ağ segmentasyonu ve mikro segmentasyon kavramlarına giriş; güvenli yapılandırma, zafiyet ve yama yönetimi; en az ayrıcalık prensibi; Zero Trust güvenlik yaklaşımına giriş; katmanlı savunma (Defense in Depth); saldırıların önlenmesi, tespit edilmesi, sınırlandırılması ve saldırı sonrası kurtarma yaklaşımları; temel siber olay müdahale süreçleri; güncel siber saldırı vakalarının saldırı ve savunma perspektifinden incelenmesi; kontrollü laboratuvar ortamlarında örnek saldırı ve savunma senaryolarının uygulanması.						
SGP1108	**Güvenli Yazılım Geliştirme ve Yazılım Güvenliği**	**Z**	**3**	**2**	**4**	**6**
Bu dersin amacı, öğrencilere yazılım yaşam döngüsünün tüm aşamalarında güvenliğin dikkate alınmasını sağlayan temel yaklaşım, yöntem ve uygulamaları öğretmektir. Öğrencilerin yazılım güvenliği risklerini tanımlayabilmesi, güvenli kod geliştirme prensiplerini uygulayabilmesi, yazılım zafiyetlerini analiz edebilmesi ve geliştirme süreçlerine güvenlik kontrollerini entegre edebilmesi hedeflenmektedir. Ayrıca öğrencilerin modern yazılım geliştirme ortamlarında DevSecOps ve yazılım tedarik zinciri güvenliğinin temel prensiplerini kavramaları amaçlanmaktadır. Ders İçeriği yazılım güvenliğinin temel kavramları ve güvenli yazılım geliştirme yaşam döngüsü (Secure SDLC); yazılım güvenliği gereksinimlerinin belirlenmesi; tehdit modelleme (Threat Modeling) ve temel risk analizi; güvenli yazılım tasarım prensipleri; güvenli kodlama (Secure Coding) ilkeleri; girdi doğrulama, çıktı kodlama ve veri doğrulama; kimlik doğrulama, yetkilendirme ve erişim kontrolü; güvenli oturum yönetimi; parola, anahtar ve gizli bilgi (secrets) yönetimi; kriptografik mekanizmaların yazılımlarda güvenli kullanımı; hata ve istisnaların güvenli yönetimi; loglama ve güvenlik açısından izlenebilirlik; yaygın yazılım zafiyetleri ve güvenlik açıklarının temel analizi; statik uygulama güvenliği testi (SAST), dinamik uygulama güvenliği testi (DAST) ve yazılım bileşimi analizi (SCA); bağımlılıkların ve üçüncü taraf yazılım bileşenlerinin güvenliği; güvenlik testleri ve zafiyet yönetimi; DevSecOps yaklaşımı ve CI/CD süreçlerinde güvenlik kontrolleri; yazılım tedarik zinciri güvenliği; Software Bill of Materials (SBOM) kavramına giriş; konteyner ve bulut tabanlı uygulama güvenliğine giriş; güvenli kod inceleme ve temel güvenlik testlerinin uygulamalı olarak gerçekleştirilmesi.						
SGP1110	**İş Sağlığı ve Güvenliği**	**Z**	**2**	**0**	**2**	**2**
Bu ders, iş sağlığı ve güvenliğinin temel kavramlarını, iş kazaları ve meslek hastalıklarının nedenlerini, risk değerlendirme yöntemlerini, işyerlerinde alınması gereken güvenlik önlemlerini ve yasal mevzuatı kapsar. Bilgisayar programcılığı alanına özgü olarak; ofis ergonomisi, ekranlı araçlarla çalışma, elektrik güvenliği, yangın güvenliği, veri merkezlerinde ve bilgisayar laboratuvarlarında karşılaşılan riskler ele alınır. Ayrıca çalışanların hak ve sorumlulukları, acil durum planları ve güvenli çalışma kültürü konularına yer verilir.						

2.SINIF III. YARIYIL

Ders Kodu	Ders Adı	Z/S	T	U	K	AKTS
SGP2101	**Siber Olay Yönetimi I**	**Z**	**3**	**0**	**3**	**4**
Bu dersin amacı, öğrencilere siber olay yönetiminin temel kavramlarını öğretmek; siber saldırıların tespit edilmesi, analiz edilmesi ve saldırılara yönelik temel müdahale süreçlerinin yürütülmesi konusunda bilgi ve beceri kazandırmaktır. Öğrencilerin saldırganların temel taktik ve tekniklerini tanıması, ağ ve sistem kayıtlarını inceleyebilmesi ve güvenlik olaylarını sınıflandırarak uygun ilk müdahale adımlarını belirleyebilmesi hedeflenmektedir. Ders içeriği siber olay ve siber saldırı kavramları; temel ağ ve bilgi güvenliği; yaygın saldırı türleri ve saldırı yaşam döngüsü; saldırgan taktik, teknik ve prosedürlerine (TTP) giriş; log kayıtlarının toplanması ve analizi; güvenlik olaylarının tespiti ve sınıflandırılması; SIEM sistemlerinin temel yapısı ve kullanımı; alarm ve olay korelasyonu; olay müdahale süreçleri; olay önceliklendirme ve eskalasyon; temel dijital delil kavramları; olay raporlama ve dokümantasyon; örnek siber olay senaryolarının incelenmesi.						
SGP2103	**Mesleki Uygulama**	**Z**	**0**	**2**	**1**	**6**
Öğrencilerin, programlarında eğitimini almış oldukları temel mesleki bilgilerini ilgilendiren işyerlerinde, uzman kişiler gözetiminde yapmış oldukları staj ile ilgili; sunum hazırlama ve sunma, hazırlanan staj defterinin staj komisyonu tarafından incelenmesi ve sorularla staj sürecinin değerlendirilmesi (eğitim alanlarıyla ilgili faaliyet gösteren kurum veya kuruluşlarda uygulamalı eğitimin alınması, mesleki konularda eğitim ve uygulama yaptırılarak iş tecrübesi kazanımı, toplam 30 iş günü staj yapılması, işyerinden gelen değerlendirme formları ile öğrencilerin yaptıkları staj sunumlarının ve hazırladıkları staj defterlerinin staj komisyonu tarafından incelenmesiyle staj değerlendirmesinin yapılması.						
SGP2105	**Proje Yönetimi Metodolojileri ve Etkili İletişim**	**Z**	**2**	**0**	**2**	**2**
Bu dersin amacı, öğrencilere iletişimde etkinlik, doğru anlatım, dinleme, sunum ve sözsüz iletişim becerilerini geliştirerek, çeşitli iletişim ortamlarında başarılı bir şekilde iletişim kurma yetenekleri kazandırmaktır. Ders içeriği proje konusu belirleme, proje süreçleri, iş akışı, proje planı oluşturma, izleme ve kontrol gibi konuları kapsamaktadır.						
SGP2107	**Kriptolojinin Temelleri**	**S**	**3**	**0**	**3**	**5**
Bu dersin amacı, öğrencilere kriptolojinin temel kavramlarını, modern kriptografik yöntemlerin çalışma prensiplerini ve bu yöntemlerin bilgi ve siber güvenlik sistemlerindeki kullanım alanlarını öğretmektir. Öğrencilerin gizlilik, bütünlük, kimlik doğrulama ve inkâr edememe gibi temel güvenlik gereksinimlerini kriptografik mekanizmalarla ilişkilendirebilmesi; simetrik ve asimetrik şifreleme, özet fonksiyonları, dijital imza ve anahtar yönetimi yaklaşımlarını kavrayabilmesi hedeflenmektedir. Ayrıca öğrencilerin kuantum hesaplamanın mevcut kriptografik sistemlere etkileri ve post-kuantum kriptografi konusunda temel farkındalık kazanmaları amaçlanmaktadır. Ders İçeriği kriptoloji, kriptografi ve kriptoanaliz kavramları; kriptografinin tarihsel gelişimi ve klasik şifreleme yöntemleri; temel sayı teorisi ve modüler aritmetiğin kriptografideki kullanımı; simetrik anahtarlı kriptografi; blok ve akış şifreleri; AES ve modern simetrik şifreleme yaklaşımları; şifreleme modları ve authenticated encryption kavramı; kriptografik özet (hash) fonksiyonları; mesaj doğrulama kodları (MAC/HMAC); parola güvenliği, salt ve anahtar türetme yaklaşımları; asimetrik anahtarlı kriptografi; RSA ve eliptik eğri kriptografisinin (ECC) temel prensipleri; anahtar değişimi; dijital imzalar; açık anahtar altyapısı (PKI), dijital sertifikalar ve sertifika otoriteleri; TLS ve güvenli iletişimde kriptografinin kullanımı; kriptografik anahtarların oluşturulması, dağıtılması, saklanması, yenilenmesi ve iptal edilmesi; rastgele sayı üretiminin kriptografik önemi; temel kriptoanaliz yaklaşımları ve kriptografik uygulama hataları; kuantum hesaplamanın mevcut kriptografik sistemlere etkileri; post-kuantum kriptografinin (PQC) temel prensipleri ve güncel standartlaşma yaklaşımlarına giriş; siber güvenlik sistemlerinde kriptografinin güncel kullanım örnekleri.						
SGP2109	**Adli Bilişim**	**S**	**3**	**0**	**3**	**5**
Bu dersin amacı, öğrencilere dijital ortamlarda meydana gelen siber olay ve suçlara ilişkin dijital delillerin belirlenmesi, korunması, elde edilmesi, incelenmesi, analiz edilmesi ve raporlanmasına yönelik temel adli bilişim bilgi ve yöntemlerini kazandırmaktır. Öğrencilerin dijital delil bütünlüğü ve delil zinciri prensiplerini kavraması; bilgisayar sistemleri, ağlar, mobil cihazlar ve bulut ortamlarından elde edilen dijital izleri temel düzeyde değerlendirebilmesi ve adli bilişim süreçlerini siber olay analiziyle ilişkilendirebilmesi hedeflenmektedir. Ders İçeriği adli bilişimin temel kavramları ve adli bilişim süreci; siber olay, siber suç ve dijital delil kavramları; dijital delillerin belirlenmesi, korunması, toplanması, elde edilmesi, incelenmesi, analiz edilmesi ve raporlanması; delil bütünlüğü ve delil zinciri (chain of custody); adli kopya (forensic image) oluşturma prensipleri; write blocker ve adli veri toplama yöntemleri; hash fonksiyonlarının dijital delil doğrulamasında kullanımı; dosya sistemleri ve dosya sistemi artefaktları; silinmiş veri ve dosyaların temel analizi; metadata ve zaman bilgileri; zaman çizelgesi (timeline) analizi; Windows ve Linux sistem artefaktları; log ve olay kayıtlarının adli analizi; tarayıcı ve internet kullanım artefaktları; e-posta ve iletişim verilerinin temel analizi; bellek (memory) adli bilişimine giriş; ağ adli bilişimine giriş ve ağ trafiğinin delil açısından değerlendirilmesi; mobil cihaz adli bilişimine giriş; bulut bilişim ortamlarında dijital delil ve bulut adli bilişiminin temel prensipleri; canlı sistemlerden veri toplama ve volatile data kavramı; zararlı yazılım ve siber saldırı olaylarında adli bilişim yaklaşımı; adli bilişim araçları ve temel kullanım prensipleri; forensic						

readiness kavramı; adli incelemelerde etik, mahremiyet ve hukuki gereklilikler; Türk hukukunda dijital delil ve bilişim suçlarının temel çerçevesi; adli bilişim bulgularının dokümantasyonu ve teknik rapor hazırlanması; örnek siber olayların adli bilişim perspektifinden incelenmesi.

SGP2111	**Yapay Zekâ ve Siber Güvenlik**	**S**	**3**	**0**	**3**	**5**

Bu dersin amacı, öğrencilere yapay zekâ ve makine öğrenmesinin temel kavramlarını öğretmek; bu teknolojilerin siber güvenlik problemlerinin tespit, analiz ve çözümünde nasıl kullanılabileceğini kavratmak ve yapay zekâ sistemlerine özgü yeni güvenlik tehditleri konusunda farkındalık kazandırmaktır. Öğrencilerin makine öğrenmesi ve üretken yapay zekâ tabanlı yaklaşımların siber tehdit tespiti, anomali analizi ve güvenlik operasyonlarındaki kullanımını anlayabilmesi; aynı zamanda yapay zekâ modellerine yönelik saldırıları ve temel savunma yaklaşımlarını değerlendirebilmesi hedeflenmektedir. Ders İçeriği yapay zekâ, makine öğrenmesi ve derin öğrenmenin temel kavramları; denetimli ve denetimsiz öğrenmeye giriş; sınıflandırma, kümeleme ve anomali tespiti; siber güvenlik verilerinin yapay zekâ ile analizi; saldırı ve zararlı davranış tespiti; ağ trafiği ve güvenlik loglarının makine öğrenmesi ile analizi; saldırı tespit sistemlerinde yapay zekâ; phishing, spam ve zararlı yazılım tespitinde makine öğrenmesi; kullanıcı ve varlık davranış analizi (UEBA); yapay zekâ destekli tehdit istihbaratı ve siber olay analizi; SOC süreçlerinde yapay zekâ ve otomasyon; adversarial machine learning kavramı; evasion ve data poisoning saldırıları; model ve veri güvenliği; yapay zekâ modellerinde gizlilik ve güvenlik riskleri; üretken yapay zekâ (Generative AI) ve büyük dil modellerinin (LLM) temel prensipleri; üretken yapay zekânın siber güvenlikte kullanımı; LLM tabanlı sistemlerde prompt injection, hassas bilgi ifşası, model/veri zehirleme ve tedarik zinciri riskleri; yapay zekâ destekli sosyal mühendislik, phishing ve deepfake tehditleri; yapay zekâ sistemlerinin güvenli ve sorumlu kullanımı; yapay zekâ güvenliğine ilişkin güncel standart, çerçeve ve yaklaşımlara giriş; siber güvenlik alanında yapay zekâ uygulamalarının örnek senaryolar üzerinden incelenmesi.

SGP2113	**Siber Güvenlik Yönetişimi**	**S**	**3**	**0**	**3**	**5**

Bu dersin amacı, öğrencilere siber güvenliğin kurumsal düzeyde yönetilmesine ilişkin temel yönetişim, risk ve uyum prensiplerini öğretmek; siber güvenlik stratejileri, politikaları, standartları ve kontrol mekanizmalarının kurumsal hedeflerle ilişkilendirilmesini kavratmaktır. Öğrencilerin siber riskleri yönetişim perspektifinden değerlendirebilmesi, temel ulusal ve uluslararası standart ve çerçeveleri tanıyabilmesi, kurumsal güvenlik politika ve sorumluluklarını anlayabilmesi ve siber güvenlik yönetişim süreçlerini temel düzeyde değerlendirebilmesi hedeflenmektedir. Ders İçeriği siber güvenlik yönetişiminin temel kavramları ve prensipleri; kurumsal yönetişim ile siber güvenlik yönetişimi arasındaki ilişki; kurumsal siber güvenlik stratejisi, politika, standart ve prosedürler; üst yönetimin siber güvenlik sorumluluğu; görev, yetki, sorumluluk ve hesap verebilirlik; siber risk yönetimi ve risk değerlendirme süreçleri; risk iştahı ve risk toleransı kavramları; bilgi varlıklarının belirlenmesi ve sınıflandırılması; erişim kontrolü ve güvenlik politikaları; ulusal ve uluslararası siber güvenlik standartları ve çerçeveleri; ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi; NIST Cybersecurity Framework (CSF) 2.0 ve Govern, Identify, Protect, Detect, Respond ve Recover fonksiyonları; COBIT yönetişim yaklaşımı; yönetişim, risk ve uyum (Governance, Risk and Compliance – GRC) kavramı; siber güvenlik kontrollerinin belirlenmesi ve değerlendirilmesi; KVKK ve siber güvenlikle ilişkili temel mevzuat; üçüncü taraf, tedarikçi ve siber tedarik zinciri risk yönetimi; siber olay yönetiminin yönetişim boyutu ve olay müdahale organizasyonu; iş sürekliliği, felaket kurtarma ve siber dayanıklılık; güvenlik denetimleri ve uyumluluk değerlendirmeleri; siber güvenlik performans göstergeleri ve temel metrikler; siber güvenlik olgunluk değerlendirmesi; siber güvenlik farkındalığı, güvenlik kültürü ve insan faktörü; bulut bilişim, yapay zekâ, IoT ve diğer gelişmekte olan teknolojilerin yönetişim ve risk yönetimine etkileri; yapay zekâ yönetişimi ve yapay zekâ kaynaklı siber risklere giriş; örnek kurumsal siber güvenlik yönetişimi ve risk senaryolarının değerlendirilmesi.

SGP2115	**Nesne Tabanlı Programlama**	**S**	**3**	**2**	**4**	**5**

Bu dersin amacı, öğrencilere nesne yönelimli programlama paradigmasının temel ve ileri kavramlarını öğretmek ve bu kavramların Python programlama dili kullanılarak yazılım geliştirme süreçlerinde uygulanabilmesini sağlamaktır. Öğrencilerin sınıf ve nesne temelli düşünme, yazılım bileşenleri arasındaki ilişkileri modelleme ve yeniden kullanılabilir, modüler, sürdürülebilir ve güvenilir yazılımlar geliştirme becerisi kazanmaları hedeflenmektedir. Ders İçeriği nesne yönelimli programlama paradigması; sınıf ve nesne kavramları; nitelikler ve metotlar; kurucular; örnek ve sınıf üyeleri; kapsülleme (encapsulation); soyutlama (abstraction); kalıtım (inheritance); çok biçimlilik (polymorphism); metot geçersiz kılma (overriding); sınıflar arası ilişkiler; bileşim (composition) ve toplama (aggregation); soyut sınıflar ve arayüz yaklaşımı; özel metotlar ve operatör aşırı yükleme; istisna yönetimi; modül ve paketlerin nesne yönelimli yapılarda kullanımı; SOLID prensiplerine giriş; temel tasarım kalıpları (design patterns); nesne yönelimli yazılımların test edilmesi; yeniden kullanılabilirlik, bakım yapılabilirlik ve kod kalitesi; nesne yönelimli yazılım tasarımı ve uygulamaları.

SGP2117	**İnternet Programlama**	**S**	**3**	**2**	**4**	**5**

Bu dersin amacı, öğrencilere internet ve web teknolojilerinin temel çalışma prensiplerini öğretmek ve modern web uygulamalarının geliştirilmesine yönelik temel bilgi ve uygulama becerileri kazandırmaktır. Öğrencilerin istemci-sunucu mimarisini anlayabilmesi; HTML, CSS ve JavaScript kullanarak etkileşimli web arayüzleri geliştirebilmesi; HTTP/HTTPS protokollerinin temel işleyişini kavrayabilmesi ve web uygulamalarında API ve veri alışverişi mekanizmalarını kullanabilmesi hedeflenmektedir. Ayrıca öğrencilerin web uygulamalarında kimlik doğrulama, oturum yönetimi ve temel

güvenli programlama prensipleri konusunda farkındalık kazanmaları amaçlanmaktadır. Ders İçeriği internet ve web teknolojilerinin temel kavramları; istemci-sunucu (client-server) mimarisi; web tarayıcıları ve web sunucularının çalışma prensipleri; HTTP ve HTTPS protokolleri; HTTP istek ve yanıt yapısı; temel HTTP metotları; HTML5 ile web sayfası yapısı ve semantik HTML; CSS ile biçimlendirme, responsive web tasarımı ve temel kullanıcı arayüzü geliştirme; JavaScript programlama temelleri ve web uygulamalarında JavaScript kullanımı; Document Object Model (DOM) ve olay yönetimi; modern JavaScript yapıları; asenkron programlama kavramı; Promise, async/await ve Fetch API kullanımı; form işlemleri ve veri doğrulama; JSON veri formatı ve web uygulamalarında veri alışverişi; REST ve RESTful API kavramları; API'lerden veri alma ve API'lerle etkileşim; frontend ve backend kavramları; sunucu taraflı programlamaya giriş; temel CRUD işlemleri; web uygulamaları ile veri tabanları arasındaki ilişkiye giriş; cookie ve session kavramları; kimlik doğrulama ve yetkilendirmeye giriş; web uygulamalarında temel güvenlik prensipleri; web uygulamalarının geliştirilmesi, test edilmesi ve yayınlanmasına ilişkin temel kavramlar; istemci-sunucu tabanlı örnek bir web uygulamasının geliştirilmesi.

2.SINIF IV. YARIYIL

Ders Kodu	Ders Adı	Z/S	T	U	K	AKTS
SGP2102	**Siber Olay Yönetimi II**	**Z**	**3**	**0**	**3**	**4**
Bu dersin amacı, öğrencilerin Siber Olay Yönetimi I dersinde edindikleri temel bilgi ve becerileri ileri düzeye taşıyarak karmaşık ve çok aşamalı siber saldırıları analiz edebilme, saldırgan davranışlarını ve saldırı zincirini ortaya çıkarabilme, gelişmiş olay müdahale süreçlerini yönetebilme ve olay sonrası iyileştirme faaliyetlerini planlayabilme yetkinliği kazanmalarını sağlamaktır. Ders İçeriği **i**leri düzey siber olay analizi; çok aşamalı saldırıların incelenmesi; saldırgan taktik, teknik ve prosedürlerinin (TTP) analizi; MITRE ATT&CK çerçevesi; gelişmiş SIEM kullanımı ve korelasyon kuralları; tehdit istihbaratının olay yönetimine entegrasyonu; Indicator of Compromise (IoC) analizi; tehdit avcılığı (Threat Hunting); uç nokta ve ağ tabanlı olay analizi; EDR/XDR yaklaşımları; dijital adli analiz ve delil yönetimi; olay müdahale senaryoları ve playbook'lar; saldırının sınırlandırılması, ortadan kaldırılması ve sistemlerin kurtarılması; olay sonrası kök neden analizi; olay sonrası değerlendirme ve raporlama; Security Operations Center (SOC) süreçleri; ileri düzey siber olay senaryoları ve uygulamaları.						
SGP2104	**Sızma Testi**	**Z**	**3**	**2**	**4**	**5**
Bu dersin amacı, öğrencilere sızma testinin temel prensiplerini, metodolojilerini ve etik-hukuki sınırlarını öğretmek; bilgi sistemleri, ağlar ve web uygulamalarındaki güvenlik açıklarının kontrollü ve yetkilendirilmiş ortamlarda belirlenmesi, doğrulanması ve raporlanmasına yönelik bilgi ve uygulama becerileri kazandırmaktır. Öğrencilerin bir sızma testi sürecini kapsam ve hedef belirlemeden keşif, zafiyet değerlendirme, kontrollü istismar ve raporlamaya kadar sistematik biçimde yürütebilmesi hedeflenmektedir. Ders İçeriği sızma testinin temel kavramları, amaçları ve türleri; sızma testi metodolojileri; etik ve hukuki sınırlar; yetkilendirme, kapsam (scope) ve Rules of Engagement (RoE); saldırı yüzeyinin belirlenmesi; pasif ve aktif bilgi toplama; açık kaynak istihbaratı (OSINT); keşif (reconnaissance), ağ tarama ve servis belirleme; Nmap ve temel ağ keşif araçları; enumeration teknikleri; zafiyet kavramı, zafiyet tarama ve zafiyet değerlendirme; CVE, CVSS ve temel zafiyet yönetimi kavramları; güvenlik açıklarının doğrulanması; kontrollü exploitation kavramı; temel sistem ve ağ sızma testleri; Windows ve Linux sistemlerine yönelik temel güvenlik testleri; parola ve kimlik doğrulama mekanizmalarının güvenlik değerlendirmesi; ayrıcalık yükseltme (privilege escalation) kavramı; Active Directory güvenlik testlerine giriş; web uygulaması ve API sızma testlerine giriş; kablosuz ağ güvenlik testlerine giriş; sosyal mühendislik saldırılarının güvenlik testi perspektifinden değerlendirilmesi; saldırı sonrası faaliyetler ve izlerin değerlendirilmesi; sızma testi bulgularının önem derecesinin belirlenmesi; teknik bulguların dokümantasyonu; risk ve düzeltme önerilerinin hazırlanması; profesyonel sızma testi raporu oluşturma; yeniden test (retest) ve doğrulama süreçleri; bug bounty ve vulnerability disclosure programlarına giriş; kontrollü laboratuvar ortamlarında örnek sızma testi senaryolarının uygulanması.						
SGP2106	**Mesleki İngilizce**	**Z**	**2**	**0**	**2**	**2**
Bu ders, öğrencilere Mesleki İngilizce becerilerini geliştirmeyi, iş dünyasında etkili iletişim kurabilmelerini sağlamayı ve Siber Güvenlik Bölümü odaklı olarak iş yazışmaları, rapor yazımı, e-posta iletişimi gibi konularda yetkinlik kazandırmayı amaçlar. Ders içeriği, İngilizce konuşma, sunum ve rapor hazırlama becerilerini geliştirmeye yönelik olarak Siber Güvenlik konularında İngilizce tartışmaları da içerir.						
SGP2108	**Bilişim Hukuku**	**S**	**3**	**0**	**3**	**4**
Bu dersin amacı, öğrencilere bilişim teknolojileri ve siber güvenlik alanında karşılaşılan temel hukuki kavram, düzenleme ve sorumlulukları öğretmek; siber olayların, bilişim suçlarının, kişisel verilerin işlenmesinin ve dijital delillerin hukuki boyutlarını değerlendirebilme becerisi kazandırmaktır. Öğrencilerin siber güvenlik faaliyetlerinin hukuki sınırlarını kavraması, kişisel verilerin korunmasına ilişkin yükümlülükleri tanıması ve güncel dijital teknolojilerin ortaya çıkardığı temel hukuki sorunlar konusunda farkındalık kazanması hedeflenmektedir. Ders İçeriği bilişim hukukunun temel kavramları, kapsamı ve kaynakları; bilgi ve iletişim teknolojilerinin hukuki boyutu; Türk hukukunda bilişim suçları ve Türk Ceza Kanunu kapsamında bilişim sistemlerine yönelik suçlar; bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme ve bilişim sistemleri aracılığıyla işlenen suçlar; 5651 sayılı Kanun ve internet ortamındaki yayınlara ilişkin temel hukuki düzenlemeler; kişisel veri ve mahremiyet kavramları; 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK); kişisel verilerin işlenmesi, saklanması, aktarılması ve korunmasına ilişkin temel yükümlülükler; özel nitelikli kişisel veriler; veri sorumlusu ve veri işleyen kavramları; kişisel veri güvenliği ve veri ihlali süreçlerinin hukuki boyutu; Avrupa Birliği Genel Veri Koruma Tüzüğü'ne (GDPR) giriş; elektronik haberleşme ve iletişim güvenliğinin hukuki boyutları; dijital delil kavramı, dijital delillerin elde edilmesi, korunması ve hukuka uygunluğu; elektronik kayıtlar ve logların delil niteliği; siber olay müdahalesinde hukuki sorumluluklar; yetkisiz erişim, güvenlik testi, zafiyet taraması ve sızma testlerinin hukuki ve etik sınırları; siber güvenlik hizmetlerinde yetkilendirme, gizlilik ve sorumluluk; elektronik imza ve elektronik işlemlerin hukuki boyutu; fikrî mülkiyet, yazılım lisansları ve açık kaynak yazılımlara ilişkin temel hukuki konular; bulut bilişim, yapay zekâ, Nesnelerin İnterneti ve yeni teknolojilerin ortaya çıkardığı temel hukuki sorunlar; yapay zekâ sistemlerinde veri, mahremiyet ve sorumluluk konuları; uluslararası siber hukuk ve sınır aşan siber olaylara giriş; siber güvenlik alanında meslek etiği; örnek bilişim hukuku ve siber olay vakalarının hukuki açıdan değerlendirilmesi.						

SGP2110	**Veri Yapıları ve Algoritma**	**S**	**3**	**0**	**3**	**4**
Bu dersin amacı, öğrencilere verilerin bilgisayar ortamında etkin biçimde düzenlenmesi, saklanması ve işlenmesinde kullanılan temel veri yapılarını ve algoritmaları öğretmek; farklı problemlere uygun veri yapısı ve algoritma seçebilme ve algoritmaların zaman ve bellek açısından verimliliğini değerlendirebilme becerisi kazandırmaktır. Öğrencilerin temel veri yapılarını uygulayabilmesi, algoritmaların performansını analiz edebilmesi ve edindiği algoritmik düşünme becerisini yazılım geliştirme ve siber güvenlik problemlerine aktarabilmesi hedeflenmektedir. Ders İçeriği veri yapıları ve algoritmalara giriş; soyut veri tipi (Abstract Data Type – ADT) kavramı; algoritma doğruluğu ve verimliliği; zaman ve alan karmaşıklığı; asimptotik analiz ve Big-O gösterimi; diziler ve dinamik diziler; bağlı listeler; tek ve çift bağlı listeler; yığın (stack), kuyruk (queue) ve çift uçlu kuyruk (deque) veri yapıları; özyineleme (recursion) ve algoritmalardaki kullanımı; arama algoritmaları; doğrusal ve ikili arama; temel sıralama algoritmaları; insertion sort, selection sort, merge sort ve quicksort; hashing kavramı; hash tabloları ve çakışma çözüm yöntemleri; ağaç veri yapıları; ikili ağaçlar ve ikili arama ağaçları; heap ve priority queue kavramları; çizge (graph) veri yapıları; çizgelerin adjacency matrix ve adjacency list ile gösterimi; çizge dolaşma algoritmaları; Breadth-First Search (BFS) ve Depth-First Search (DFS); en kısa yol ve minimum kapsayan ağaç problemlerine giriş; Dijkstra, Prim ve Kruskal algoritmalarının temel prensipleri; brute force, divide-and-conquer ve greedy gibi temel algoritma tasarım yaklaşımları; veri yapısı ve algoritma seçiminde zaman-bellek dengesi; farklı veri yapısı ve algoritmaların performanslarının karşılaştırılması; veri yapıları ve algoritmaların yazılım ve siber güvenlik problemlerindeki temel uygulamaları.					
SGP2112	**Bulut Teknolojileri**	**S**	**3**	**0**	**3**	**4**
Bu dersin amacı, öğrencilere sanallaştırma ve bulut bilişim teknolojilerinin temel kavramlarını, mimarilerini ve hizmet modellerini öğretmek; bulut ortamlarının yönetimi ve güvenliğine ilişkin temel bilgi ve farkındalık kazandırmaktır. Öğrencilerin bulut bilişim altyapılarını, hizmet ve dağıtım modellerini, sanallaştırma ve konteyner teknolojilerini anlayabilmesi; bulut ortamlarında kimlik ve erişim yönetimi, veri güvenliği, ağ güvenliği, izleme ve olay yönetimi gibi temel güvenlik süreçlerini değerlendirebilmesi hedeflenmektedir. Ders İçeriği bulut bilişimin temel kavramları ve gelişimi; sanallaştırma teknolojileri; hipervizörler, sanal makineler, sanal ağlar ve sanal depolama; bulut bilişim mimarileri; IaaS, PaaS ve SaaS hizmet modelleri; genel, özel, hibrit ve çoklu bulut (multi-cloud) yaklaşımları; bulut kaynaklarının oluşturulması, yönetilmesi ve ölçeklendirilmesi; bulut depolama ve veri yönetimi; konteyner (container) teknolojilerine giriş; Docker ve Kubernetes'in temel kavramları; cloud-native uygulama ve mikroservis mimarilerine giriş; bulut bilişimde paylaşılan sorumluluk modeli (Shared Responsibility Model); bulut ortamlarında kimlik ve erişim yönetimi (IAM); rol tabanlı erişim ve en az ayrıcalık prensibi; bulut ağlarının temel yapısı, ağ segmentasyonu ve güvenliği; bulut ortamlarında veri güvenliği ve şifreleme; anahtar ve gizli bilgi (secrets) yönetimine giriş; güvenli yapılandırma ve yanlış yapılandırma (misconfiguration) riskleri; bulut ortamlarında zafiyet ve yama yönetimi; konteyner ve bulut iş yükü güvenliğine giriş; bulut loglarının toplanması, izlenmesi ve güvenlik açısından değerlendirilmesi; bulut güvenlik izleme ve tehdit tespiti; bulut ortamlarında yedekleme, iş sürekliliği ve felaket kurtarma; bulut ortamlarında olay müdahalesi ve bulut adli bilişimine giriş; Zero Trust yaklaşımının bulut ortamlarındaki yeri; bulut güvenliğine ilişkin temel standart, iyi uygulama ve uyumluluk yaklaşımları; güncel bulut bilişim ve bulut güvenliği senaryolarının incelenmesi.					
SGP2114	**Yeni Nesil Teknolojiler**	**S**	**3**	**0**	**3**	**4**
Bu dersin amacı, öğrencilere bilgi ve iletişim teknolojilerinde ortaya çıkan yeni ve gelişmekte olan teknolojileri tanıtmak; bu teknolojilerin temel çalışma prensiplerini, kullanım alanlarını ve siber güvenlik üzerindeki etkilerini değerlendirebilme becerisi kazandırmaktır. Öğrencilerin yapay zekâ, blokzincir, kuantum teknolojileri, yeni nesil haberleşme sistemleri, Nesnelerin İnterneti, uç bilişim ve diğer gelişmekte olan teknolojilerin oluşturduğu yeni saldırı yüzeylerini, güvenlik gereksinimlerini ve gelecekteki siber güvenlik yaklaşımlarını temel düzeyde analiz edebilmesi hedeflenmektedir. Ders İçeriği yeni ve gelişmekte olan teknolojiler kavramı ve teknolojik dönüşüm; yeni teknolojilerin siber güvenlik ekosistemine etkileri; yapay zekâ ve üretken yapay zekâ teknolojilerine genel bakış; yapay zekâ destekli sistemlerin güvenlik fırsatları ve oluşturduğu yeni tehditler; otonom ve yapay zekâ ajanlı sistemlere giriş; blokzincir ve dağıtık defter teknolojilerinin temel prensipleri; akıllı sözleşmeler ve blokzincir güvenliğine giriş; Nesnelerin İnterneti (IoT) ve Endüstriyel Nesnelerin İnterneti (IIoT); IoT cihaz, haberleşme ve veri güvenliği; uç bilişim (Edge Computing) ve dağıtık bilişim mimarileri; 5G ve 6G haberleşme teknolojilerinin temel özellikleri ve güvenlik boyutları; yazılım tanımlı ve sanallaştırılmış iletişim altyapılarına giriş; siber-fiziksel sistemler ve kritik altyapı güvenliği; dijital ikiz (Digital Twin) teknolojileri ve güvenlik riskleri; artırılmış gerçeklik, sanal gerçeklik ve genişletilmiş gerçeklik (AR/VR/XR) sistemlerinin güvenlik ve mahremiyet boyutları; kuantum hesaplamanın temel kavramları; kuantum hesaplamanın mevcut siber güvenlik ve kriptografik sistemlere etkileri; kuantum tehdidi ve post-kuantum kriptografiye (PQC) giriş; kuantuma dayanıklı sistemlere geçiş ve kriptografik çeviklik (crypto-agility) kavramı; yeni nesil kimlik ve erişim teknolojileri; gelişmekte olan teknolojilerde veri güvenliği, mahremiyet ve etik sorunlar; yeni teknolojilerin oluşturduğu saldırı yüzeyleri ve tehdit modelleri; gelişmekte olan teknolojilerin siber güvenlik açısından risk, fırsat ve stratejik etkilerinin güncel örnekler üzerinden değerlendirilmesi.					
SGP2116	**Web ve Uygulama Güvenliği**	**S**	**2**	**2**	**3**	**4**
Bu dersin amacı, öğrencilere modern web ve uygulama mimarilerinde ortaya çıkan güvenlik risklerini tanıma, yaygın güvenlik açıklarını analiz etme, temel güvenlik testlerini gerçekleştirme ve tespit edilen zafiyetlere yönelik güvenli çözüm						

yaklaşımlarını değerlendirme becerisi kazandırmaktır. Öğrencilerin web uygulamaları ve API'lerde kimlik doğrulama, yetkilendirme, oturum ve veri güvenliği mekanizmalarını anlayabilmesi; güncel web güvenliği zafiyetlerini kontrollü laboratuvar ortamlarında inceleyebilmesi ve uygulama güvenliğinin artırılmasına yönelik temel önlemleri uygulayabilmesi hedeflenmektedir. Ders İçeriği Web ve uygulama güvenliğinin temel kavramları; modern web uygulama mimarileri ve istemci-sunucu iletişiminin güvenlik açısından incelenmesi; HTTP/HTTPS güvenliği; TLS'in web uygulamalarındaki rolü; HTTP başlıkları ve güvenlik başlıkları; cookie ve oturum güvenliği; SameSite, Secure ve HttpOnly özellikleri; OWASP Top 10 ve güncel web uygulaması risk kategorileri; girdi doğrulama ve çıktı kodlama; SQL Injection ve diğer injection zafiyetleri; Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF); Server-Side Request Forgery (SSRF); path traversal ve dosya işlemlerine ilişkin güvenlik açıkları; güvenli ve güvensiz dosya yükleme mekanizmaları; kimlik doğrulama ve yetkilendirme zafiyetleri; erişim kontrolü ve Broken Access Control; parola güvenliği ve çok faktörlü kimlik doğrulama; oturum yönetimi zafiyetleri; CORS ve Content Security Policy (CSP) kavramları; RESTful API güvenliği; OWASP API Security risklerine giriş; API'lerde kimlik doğrulama, yetkilendirme, veri doğrulama ve erişim kontrolü; token tabanlı kimlik doğrulama; JWT, OAuth 2.0 ve OpenID Connect'in temel güvenlik prensipleri; istemci tarafı ve JavaScript tabanlı uygulamalarda temel güvenlik riskleri; üçüncü taraf kütüphaneler, bağımlılıklar ve yazılım tedarik zincirinden kaynaklanan uygulama güvenliği riskleri; hassas verilerin korunması ve kriptografik mekanizmaların web uygulamalarında doğru kullanımı; hata mesajları, loglama ve güvenlik açısından izlenebilirlik; web uygulaması saldırı yüzeyinin belirlenmesi; zafiyet tarama ve temel web güvenlik testleri; proxy tabanlı web güvenliği analiz araçlarının kullanımı; statik ve dinamik uygulama güvenliği testlerine giriş; güvenlik bulgularının değerlendirilmesi, önem derecelendirilmesi ve raporlanması; tespit edilen zafiyetlerin giderilmesi ve güvenli kodlama yaklaşımları; kontrollü laboratuvar ortamlarında web ve API güvenliği uygulamaları.

SGP2118	**Zararlı Yazılım Analizi ve Tespiti**	**S**	**2**	**2**	**3**	**4**

Bu dersin amacı, öğrencilere zararlı yazılımların temel türlerini, çalışma mekanizmalarını ve sistemler üzerindeki davranışlarını öğretmek; zararlı yazılımların güvenli ve kontrollü ortamlarda statik ve dinamik yöntemlerle incelenmesi, tespit edilmesi ve analiz bulgularının değerlendirilmesine yönelik temel bilgi ve uygulama becerileri kazandırmaktır. Öğrencilerin zararlı yazılım davranışlarını sistem ve ağ üzerindeki izlerden belirleyebilmesi, temel analiz yöntem ve araçlarını kullanabilmesi, güvenlik göstergeleri (IoC) çıkarabilmesi ve analiz sonuçlarını siber olay müdahale süreçleriyle ilişkilendirebilmesi hedeflenmektedir. Ders İçeriği zararlı yazılım kavramı, gelişimi ve sınıflandırılması; virüs, solucan, truva atı, spyware, rootkit, bot/botnet, ransomware ve diğer zararlı yazılım türleri; dosya tabanlı ve dosyasız (fileless) zararlı yazılımlar; zararlı yazılımların bulaşma, çalıştırılma, kalıcılık (persistence) ve yayılma mekanizmaları; Windows işletim sistemi ve zararlı yazılım ilişkisi; Windows Portable Executable (PE) dosya yapısına giriş; x86/x64 mimarisi ve Assembly dilinin zararlı yazılım analizi açısından temel kavramları; zararlı yazılım analiz süreci ve güvenli analiz laboratuvarının oluşturulması; sanal makineler, izole ortamlar ve sandbox teknolojileri; temel statik analiz yöntemleri; dosya türü, hash, string, metadata ve PE bilgilerinin incelenmesi; temel dinamik ve davranışsal analiz; süreç, dosya sistemi, kayıt defteri ve ağ faaliyetlerinin izlenmesi; sistem çağrıları ve süreç davranışlarının temel analizi; bellek analizine giriş; zararlı yazılımlarda kod gizleme (obfuscation), packing ve temel anti-analysis teknikleri; zararlı ağ trafiğinin incelenmesi; Command and Control (C2) iletişimi kavramı; Indicator of Compromise (IoC) belirleme ve çıkarma; hash, dosya, süreç, alan adı, IP adresi ve diğer güvenlik göstergelerinin değerlendirilmesi; YARA kurallarının temel yapısı ve zararlı yazılım tespitinde kullanımı; zararlı yazılım davranışlarının MITRE ATT&CK taktik ve teknikleriyle ilişkilendirilmesi; antivirüs, EDR ve diğer uç nokta güvenlik teknolojilerinin zararlı yazılım tespitindeki rolü; ransomware ve güncel zararlı yazılım vakalarının analizi; temel tersine mühendislik yaklaşımı; zararlı yazılım analiz sonuçlarının dokümantasyonu ve teknik raporlanması; kontrollü laboratuvar ortamlarında statik ve dinamik zararlı yazılım analizi uygulamaları.

SGP2120	**Veri Tabanı Uygulamaları ve Güvenliği**	**S**	**2**	**2**	**3**	**4**

Bu dersin amacı, öğrencilere veri tabanı sistemlerinin temel kavramlarını, veri modelleme ve sorgulama yöntemlerini öğretmek; veri tabanlarının güvenli biçimde tasarlanması, yapılandırılması, yönetilmesi ve izlenmesine yönelik temel bilgi ve uygulama becerileri kazandırmaktır. Öğrencilerin ilişkisel veri tabanlarını tasarlayabilmesi ve SQL kullanarak veri işlemleri gerçekleştirebilmesinin yanı sıra, veri tabanlarına yönelik temel güvenlik tehditlerini tanıyabilmesi, erişim kontrolü ve veri koruma mekanizmalarını uygulayabilmesi hedeflenmektedir. Ders İçeriği veri tabanı sistemlerinin temel kavramları ve mimarileri; veri modelleri; ilişkisel veri tabanı modeli; varlık-ilişki (ER) modelleme; tablolar, anahtarlar ve ilişkiler; normalizasyonun temel prensipleri; ilişkisel cebire giriş; Yapısal Sorgu Dili (SQL); veri tanımlama (DDL), veri işleme (DML) ve veri kontrol (DCL) komutları; SELECT sorguları, filtreleme, sıralama, gruplama, alt sorgular ve JOIN işlemleri; transaction kavramı ve ACID özellikleri; veri bütünlüğü ve kısıtlamalar; ilişkisel olmayan (NoSQL) veri tabanlarına giriş ve temel kullanım alanları; veri tabanı güvenliğinin temel prensipleri; veri tabanı kullanıcıları, roller ve yetkilendirme; kimlik doğrulama ve erişim kontrolü; rol tabanlı erişim kontrolü (RBAC) ve en az ayrıcalık prensibi; SQL Injection ve temel veri tabanı saldırıları; parametrik sorgular ve güvenli veri tabanı erişimi; veri tabanlarının güvenli yapılandırılması ve hardening prensipleri; veri tabanı hesapları ve kimlik bilgilerinin güvenliği; hassas verilerin korunması; durağan ve aktarım halindeki verilerin şifrelenmesi; anahtar ve gizli bilgi yönetimine giriş; veri tabanı logları, auditing ve güvenlik izleme; şüpheli veri tabanı faaliyetlerinin temel analizi; yedekleme, geri yükleme ve veri dayanıklılığı; veri tabanlarında zafiyet, güncelleme ve yama yönetimi; bulut tabanlı veri tabanı hizmetlerine giriş ve bulut veri tabanı güvenliği; veri tabanı güvenliğinde paylaşılan

sorumluluk yaklaşımı; kişisel ve hassas verilerin korunmasına ilişkin temel güvenlik gereksinimleri; veri tabanı güvenliği olaylarının ve örnek saldırı senaryolarının kontrollü ortamlarda incelenmesi.						
SGP2122	**Mobil Teknolojiler ve Güvenlik**	**S**	**2**	**2**	**3**	**4**
Bu dersin amacı, öğrencilere mobil cihazların, mobil işletim sistemlerinin ve mobil uygulamaların temel güvenlik mimarilerini öğretmek; mobil ortamlardaki güvenlik tehditlerini, zafiyetleri ve koruma mekanizmalarını analiz edebilme becerisi kazandırmaktır. Öğrencilerin Android ve iOS platformlarının temel güvenlik mekanizmalarını anlayabilmesi, mobil uygulamalardaki yaygın güvenlik risklerini belirleyebilmesi, mobil cihaz ve uygulamalara yönelik temel güvenlik analizlerini kontrollü ortamlarda gerçekleştirebilmesi ve mobil güvenliği kurumsal siber güvenlik süreçleriyle ilişkilendirebilmesi hedeflenmektedir. Ders İçeriği mobil teknolojilerin ve mobil güvenliğin temel kavramları; mobil cihaz ve mobil uygulama ekosistemleri; Android ve iOS işletim sistemlerinin temel mimarileri ve güvenlik modelleri; uygulama sandboxing ve izolasyon mekanizmaları; mobil uygulama izinleri ve yetkilendirme modelleri; uygulama imzalama ve güven zinciri; mobil cihazlarda kimlik doğrulama, biyometrik doğrulama ve erişim kontrolü; mobil cihazlarda veri güvenliği; güvenli veri depolama, şifreleme ve anahtar yönetimine giriş; mobil uygulamalarda hassas veri ve kimlik bilgilerinin korunması; mobil ağ iletişimi ve güvenli haberleşme; TLS ve sertifika doğrulamanın mobil uygulamalardaki rolü; mobil uygulama ile backend/API arasındaki iletişimin güvenliği; Android ve iOS uygulamalarındaki yaygın güvenlik zafiyetleri; OWASP Mobile Application Security yaklaşımı ve güncel mobil uygulama güvenliği riskleri; mobil uygulamaların statik ve dinamik güvenlik analizine giriş; mobil uygulama paketlerinin ve temel artefaktların incelenmesi; mobil uygulamalarda tersine mühendislik kavramına giriş; root ve jailbreak kavramları ve bunların güvenlik etkileri; mobil zararlı yazılımlar, spyware ve güncel mobil tehditler; phishing, smishing ve mobil sosyal mühendislik tehditleri; güvenli olmayan kablosuz bağlantılar, Bluetooth, NFC ve diğer mobil iletişim teknolojilerinden kaynaklanan temel güvenlik riskleri; mobil cihaz yönetimi (MDM) ve kurumsal mobil güvenlik; BYOD güvenliği; Mobile Threat Defense (MTD) yaklaşımına giriş; mobil cihazlarda güvenlik logları, olay tespiti ve olay müdahalesine giriş; kayıp veya ele geçirilmiş mobil cihazlara ilişkin güvenlik süreçleri; mobil cihaz adli bilişimine giriş; mobil uygulama gizliliği, izinler ve kişisel verilerin korunması; Android ve iOS ortamlarında temel mobil güvenlik analizlerinin kontrollü laboratuvar uygulamaları.						