

Dersin Adı	Kodu	Yarıyılı	T+U	Kredisi	AKTS
Siber Güvenlik		8	3+0	3	6
Ön koşul Dersler	Yok				
Dersin Dili	Türkçe				
Dersin Seviyesi	Lisans				
Dersin Türü	Seçmeli				
Dersin Koordinatörü					
Dersi Veren					
Dersin Yardımcıları					
Dersin Amacı	Bilgi sistemlerinin değerlendirilmesi amacıyla düşman davranış simülasyonları. Saldırıların adli analizi için test sistemlerinde farklı sistemlerin ve savunma tekniklerinin incelenmesi. Zayıflıkların azaltılması ve tehditlere karşı durabilmek için mühendislik çözümleri geliştirilmesi. Bilgi güvenliği amaçları bakımından farklı zayıf ve güçlü yönlerin tespit edilmesi, sızma testleri, tehdit modelleme, zafiyet analizi, kötüye kullanım ve raporlama.				
Dersin Öğrenme Çıktıları	<b>Bu dersin sonunda öğrenci;</b> 1- Siber güvenlik operasyonlarının tanımlayan bileşenleri anlayabilmek. 2- Verimli siber güvenlik operasyonlarını tanımlayabilmek. 3- Zayıf noktaları azaltmak ve tehlikelerle baş edebilmek için çözümler geliştirebilmek.				
Dersin İçeriği	Siber güvenlik ve Güvenlik Operasyon Merkezleri, İşletim Sistemleri: Windows İşletim Sistemi, Linux İşletim Sistemi. Ağ protokolleri ve servisleri. Ağ altyapısı. Ağ güvenliğinin prensipleri, Ağ saldırıları. Ağ koruması. Kriptografi ve Açık Anahtarlama Altyapısı. Uç nokta güvenliği ve analizi. Güvenlik izleme. Ağ güvenliği ve dijital deliller.				
<b>Haftalar</b>	<b>Konular</b>				
1	Giriş				
2	Siber güvenlik ve Güvenlik Operasyon Merkezleri				
3	İşletim Sistemleri: Windows İşletim Sistemi				
4	Linux İşletim Sistemi				
5	Ağ Protokolleri ve Servisleri				
6	Ağ altyapısı				
7	Ağ güvenliği prensipleri				
8	Ağ saldırıları				
9	Ağın Korunması				
10	Kriptografi ve Açık Anahtarlama Altyapısı				
11	Uç nokta güvenliği ve analizi				
12	Güvenlik izleme				
13	Ağ güvenliği ve dijital deliller				
14	Raporlama				
<b>Genel Yeterlilikler</b>					
1- Siber güvenlik alanındaki konseptleri ifade edebilir. 2- Bilişim hukuku, uluslararası standartlar ve karşı tedbirlerin siber güvenlikle ilişkisini izah edebilir. 3- Bilgisayar suçları ve ağ güvenliğinin konularındaki temel bilgileri hatırlar.					
<b>Kaynaklar</b>					
Rittinghouse, J., Hancock, W. M., & CISSP, C. (2003). <i>Cybersecurity operations handbook</i> . Digital Press. Altınkaynak, M. (2017). <i>Uygulamalı Siber Güvenlik ve Hacking</i> , Abaküs Bookstore, İstanbul. Akyıldız, M.A. (2020). <i>Uygulamalarla Siber Güvenliğe Giriş</i> , Gazi Kitabevi, İstanbul.					
<b>Değerlendirme Sistemi</b>					
Dönem başında ders izlençe formunda ilan edilir.					

<b>PROGRAM ÖĞRENME ÇIKTILARI İLE DERS ÖĞRENİM KAZANIMLARI İLİŞKİSİ TABLOSU</b>											
	<b>PÇ1</b>	<b>PÇ2</b>	<b>PÇ3</b>	<b>PÇ4</b>	<b>PÇ5</b>	<b>PÇ6</b>	<b>PÇ7</b>	<b>PÇ8</b>	<b>PÇ9</b>	<b>PÇ10</b>	<b>PÇ11</b>
<b>ÖK1</b>	2	3	4	2	3						
<b>ÖK2</b>	2	4	3	4	1						
<b>ÖK3</b>	2	4	3	3	3						
<b>ÖK: Öğrenme Çıktıları PÇ: Program Çıktıları</b>											
<b>Katkı Düzeyi</b>	<b>1 Çok Düşük</b>		<b>2 Düşük</b>		<b>3 Orta</b>		<b>4 Yüksek</b>		<b>5 Çok Yüksek</b>		
<b>Program Çıktıları ve İlgili Dersin İlişkisi</b>											
	<b>PÇ1</b>	<b>PÇ2</b>	<b>PÇ3</b>	<b>PÇ4</b>	<b>PÇ5</b>	<b>PÇ6</b>	<b>PÇ7</b>	<b>PÇ8</b>	<b>PÇ9</b>	<b>PÇ10</b>	<b>PÇ11</b>
Siber Güvenlik	2	4	3	3	2						