DERS TANITIM ve UYGULAMA BİLGİLERİ

Dersin Adı	Kodu	Yarıyıl	T+U+L (saat/hafta)	Türü (Z / S)	Yerel Kredi	AKTS
Dijital Forensik ve Olay İnceleme	CCIP 523	Bahar	03+00+00	Zorunlu	3	7.5

Akademik Birim:	Siber Güvenlik
Öğrenim Türü:	Örgün Eğitim
Ön Koşullar	Yok
Öğrenim Dili:	İngilizce
Dersin Düzeyi:	Yüksek Lisans
Dersin Koordinatörü:	Mahmut Çavur
Dersin Amacı:	Olay müdahale ekipleri ve tehdit avcıları, gelişmiş tehditleri tespit etmek, izlemek ve içermek ve olayları düzeltmek için en son araçlar, bellek analiz teknikleri ve kurumsal metodolojilerle donanmalıdır. Olay tepkisi ve tehdit avı analistleri analizlerini işletmelerindeki binlerce sistem arasında ölçeklendirebilmelidir.
Dersin İçeriği:	Öğrenciler, kurumdaki yüzlerce veya binlerce sistemdeki eylemleri bağlamak ve kodlamak için iş istasyonlarını veya SIFT iş istasyonlarını kullanmalarını sağlayan tam bir F-Response Enterprise Edition eğitimi alacaklardır. Bu özellik, yeni olay yanıtını karşılaştırmak, kolaylaştırmak ve göstermek ve yanıt verenlerin tüm işletme ağı genelinde uzlaşma göstergelerini aramasını sağlayan tehdit avı teknolojilerini tehdit etmek için kullanılır.
Dersin Öğrenme Çıktıları (ÖÇ):	• **1-** Bir ihlalin nasıl ve ne zaman gerçekleştiğini tespit etme. • **2-** Etkilenen ve etkilenen sistemleri tanımlamak. • **3-** Hasar değerlendirmeleri yapma ve neyin çalındığını veya değiştirildiğini belirleme. • **4-** Olayları içerme ve giderme. • **5-** Tehdit istihbaratının temel kaynaklarını geliştirme.
Dersin Öğrenme Yöntem ve Teknikleri	Sınıf dersleri, ödevler, vize ve final sınavları, Laboratuar uygulamaları.

HAFTALIK PROGRAM

Hafta	Konular	Ön Hazırlık
1	Giriş	
2	Gerçek Olay Müdahale Taktikleri	
3	Tehdit Avı	
4	Siber Tehdit İstihbaratı	
5	Siber Tehdit İstihbaratı	
6	Kötü Amaçlı Yazılım Savunmasının Kaçakçılığı ve Tanımlanması	
7	Kötü Amaçlı Yazılım Savunmasının Kaçakçılığı ve Tanımlanması	
8	Arasınav	
9	Kötü Amaçlı Yazılım Kalıcılığı Kimliği	
10	Uzaktan ve Kurumsal Olay Tepkisi	
11	Müdahale ve Avcılıkta Bellek Adli Analiz Analizi	
12	Hafıza Adli Muayeneleri	
13	lay Müdahaleleri ve Avcılar İçin Olay Günlüğü Analizi	

14	Dönem Sonu Sınav çalışmaları	Dönem içi konuların tekrarı

Kadir Has Üniversitesi'nde bir dönem 14 haftadır, 15. ve 16. hafta sınav haftalarıdır.

ZORUNLU ve ÖNERİLEN OKUMALAR

''Introduction to Computer Security'' by Matt Bishop, Pearson Publications.

DİĞER KAYNAKLAR

-

DEĞERLENDİRME SİSTEMİ

Yarıyıl İçi Çalışmaları	**Sayı**	**Katkı Payı (%)**
Proje	1	10
Ödev	3	15
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	5	35
Final Sınavı	1	40
Total:	**10**	**100**

İŞ YÜKÜ HESAPLAMASI

Etkinlikler	**Sayısı**	**Süresi (saat)**	**Toplam İş Yükü (saat)**
Ders Saati	14	3	42
Proje	1	20	20
Ödev	3	15	45
Dersle İlgili Sınıf Dışı Etkinlikler	9	3	27
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	1	40	40
Final Sınavı	1	25	25
Toplam İş Yükü (saat):			**199**

1 AKTS = 25 saatlik iş yükü

PROGRAM YETERLİLİKLERİ (PY) ve ÖĞRENME ÇIKTILARI (ÖÇ) İLİŞKİSİ

#	PY1	PY2	PY3	PY4	PY5	PY6	PY7	PY8	PY9	PY10	PY11	PY12

OC1				1			2				3	
OC2				1			2				3	
OC3				1			2				3	
OC4				1			2				3	
OC5				1			2				3	

Katkı Düzeyi: 1 Düşük, 2 Orta, 3 Yüksek