TOROS ÜNİVERSİTESİ

Meslek Yüksekokulu
Bilgi Güvenliği Teknolojisi

Ders Bilgileri

GÜVENLİK OLAY YÖNETİMİ					
Kodu	**Dönemi**	**Teori**	**Uygulama**	**Ulusal Kredisi**	**AKTS Kredisi**
		Saat / Hafta			
BGT108	Bahar	3	0	3	

Ön Koşulu Olan Ders(ler)	
Dili	Türkçe
Türü	Zorunlu
Seviyesi	Ön Lisans
Öğretim Elemanı(ları)	Öğr. Gör. Özer TANRIVERDİ
Öğretim Sistemi	Yüz Yüze
Önerilen Hususlar	
Staj Durumu	Yok
Amacı	Log, loglama ve log yönetimi kavramlarını öğrenme, SIEM ürünlerinin neler olduğunu öğrenme, Splunk yazılımını kurma, temel özelliklerini öğrenme, Splunk'ta log yükleme, arama yapma, raporlama, alert özelliğini kullanma, universal forwarder'lar kullanarak uzak sistemlerden log yükleme, siber güvenlik genel tanım ve kavramlarını öğrenme, siber olaylara müdahale süreçlerini ve bu süreçlerde kullanılan araçları öğrenme, adli bilişim kavramını ve imaj almayı öğrenme, zararlı yazılımları inceleme yöntemlerini öğrenme.
İçeriği	Log kavramı, loglama ve log yönetimi, SIEM ürünleri, Splunk yazılımı, Splunk'ta log yükleme, arama ve operatör kullanma, raporlama ve analiz, alert özelliği, universal forwarder'lar, siber güvenlik genel tanım ve kavramlar, siber olaylara müdahale süreçleri, siber olaylara müdahale sürecinde kullanılan araçlar, adli bilişim, imaj alma ve zararlı yazılımların incelenmesi.

Dersin Öğrenim Çıktıları

#	Öğrenim Çıktıları
1	Log, loglama ve log yönetimi kavramlarını öğrenme
2	Splunk yazılımını tanıma, Splunk'ta log yüklemeyi, arama yapmayı, raporlamayı, alert özelliğini kullanmayı, uzak sistemlerden log yüklemeyi öğrenme
3	Siber Güvenlik genel tanım ve kavramları öğrenme
4	Siber Olaylara müdahale süreçlerini ve bu süreçlerde kullanılan araçların neler olduğunu öğrenme
5	Adli Bilişim, imaj alma ve zararlı yazılımları incelemeyi öğrenme

Haftalık Ayrıntılı Ders İçeriği

#	Konular	Öğretim Yöntem ve Teknikleri
1	Log ve loglama nedir, temel özellikleri nelerdir?	Anlatım, örnekler
2	Log yönetimi ve SIEM ürünleri	Anlatım, örnekler
3	Splunk yazılımı kurulumu ve temel özellikleri	Anlatım, örnekler, uygulama
4	Splunk'ta log yükleme yöntemleri	Anlatım, örnekler, uygulama
5	Splunk'ta log arama ve operatör kullanımı	Anlatım, örnekler, uygulama
6	Splunk'ta raporlama ve analiz	Anlatım, örnekler, uygulama
7	Splunk'ta alert özelliği	Anlatım, örnekler, uygulama
8	Ara Sınav	Sınav
9	Splunk'ta universal forwarder'lar	Anlatım, örnekler, uygulama

10	Siber güvenlikte genel tanımlar ve kavramlar	Anlatım, örnekler
11	Siber olaylara müdahale süreçleri	Anlatım, örnekler
12	Siber olaylara müdahale sürecinde kullanılan araçlar	Anlatım, örnekler
13	Adli bilişim, imaj alma ve zararlı yazılımların incelenmesi	Anlatım, örnekler
14	Son Sınav	Sınav
15		
16		

Resources

#	Malzeme / Kaynak Adı	Kaynak Hakkında Bilgi	Referans / Önerilen Kaynak
1	Logging and Log Management, Dr. Anton A. Chuvakin, Kevin J. Schmidt, Christopher Phillips		
2	Siber Güvenlik ve Savunma, Farkındalık ve Caydırıcılık, Editörler: Prof. Dr. Şeref Sağıroğlu, Prof. Dr. Mustafa Alkan		

Ölçme ve Değerlendirme Sistemi

#	Ağırlık	Çalışma Türü	Çalışma Adı
1	%40	Ara Sınav	Ara Sınav
2	%60	Son Sınav	Son Sınav

Dersin Öğrenim Çıktıları ve Program Yeterlilikleri ile İlişkileri

#	Öğrenim Çıktıları	Program Çıktıları	Ölçme ve Değerlendirme
1	Log, loglama ve log yönetimi kavramlarını öğrenme	1,4,5	
2	Splunk yazılımını tanıma, Splunk'ta log yüklemeyi, arama yapmayı, raporlamayı, alert özelliğini kullanmayı, uzak sistemlerden log yüklemeyi öğrenme	1,4,5	
3	Siber Güvenlik genel tanım ve kavramları öğrenme	1,4,5	
4	Siber Olaylara müdahale süreçlerini ve bu süreçlerde kullanılan araçların neler olduğunu öğrenme	1,4,5	
5	Adli Bilişim, imaj alma ve zararlı yazılımları incelemeyi öğrenme	1,4,5	

Not: Ölçme ve Değerlendirme sütununda belirtilen sayılar, bir üstte bulunan Ölçme ve Değerlerndirme Sistemi başlıklı tabloda belirtilen çalışmaları işaret etmektedir.

İş Yükü Detayları

#	Etkinlik	Adet	Süre (Saat)	İş Yükü
1	Ders Süresi	14	3	42
2	Sınıf Dışı Ders Süresi (Ön çalışma, pekiştirme)	14	2	28
3	Sunum ve Seminer Hazırlama	0	0	0
4	İnternette tarama, kütüphane ve arşiv çalışması	0	0	0
5	Belge/Bilgi listeleri oluşturma	0	0	0
6	Atölye	0	0	0
7	Ara Sınav için Hazırlık	1	8	8
8	Ara Sınav	1	1	1
9	Kısa Sınav	0	0	0
10	Ödev	0	0	0
11	Ara Proje	0	0	0

12	Ara Uygulama	0	0	0
13	Son Proje	0	0	0
14	Son Uygulama	0	0	0
15	Son Sınav için Hazırlık	1	10	10
16	Son Sınav	1	1	1
				90