SAO 202/SAO 202E SİBER OLAY YÖNETİMİ

DERS PLANI

Hafta	Konular
1	Siber Olay Yönetiminin İlkeleri
2	Siber Saldırı Türleri
3	Siber Olayların Tespiti ve Analizi
4	Merkezi Kayıt ve Yönetim Sistemleri
5	Olay İlişkilendirme Sistemleri (SIM)
6	Bilgi Güvenliği ve Olay Yönetimi (SIEM)
7	Adli Bilişim
8	Arasınav
9	SIEM Araçları
10	Siber Olaylara Müdahele Ekipleri (SOME)
11	SOME Operasyonel Elemanları ve Proje Planı
12	Açık Kaynak Kodlu Merkezi Güvenlik İzleme Yazılımı (OSSIM)
13	Log Analizi
14	SOC Lab. Çalışması Seviye1 - Olay Müdahale Senaryo Uygulamaları & SOC Lab. Çalışması Seviye1
15	-
16	Final Sınavı

COURSE PLAN

Weeks	Topics
1	Principles of Cyber Incident Management
2	Types of Cyber Attacks
3	Detection and Analysis of Cyber Incidents
4	Centralized Logging and Management Systems
5	Incident Correlation Systems (SIM)
6	Information Security and Incident Management (SIEM)
7	Digital Forensics
8	Midterm Exam
9	SIEM Tools
10	Cyber Incident Response Teams (CIRTs)
11	Operational Elements of CIRTs and Project Planning
12	Open Source Central Security Monitoring Software (OSSIM)
13	Log Analysis
14	SOC Lab Work Level 1 - Incident Response Scenario Applications & SOC Lab Work Level 1
15	-
16	Final Exam