ALTAY TAKIMI
EĞİTİM İÇERİĞİ RAPORU

HAZIRLAYAN: GÜRKAN PARLAK

İçindekiler

Rapor İçeriği

Bu rapor siber olaylara müdahele ve defans alanında çalışmalar yapan Altay Takımı için eğitim içeriği yol haritası olarak hazırlanmıştır.
Bu anlamda kısaca bu rapor hazırlanana kadar geçen süreçte Altay Takımı'nın yaptığı çalışmaları kısaca açıklayalım:

Antalya Bootcamp İşlenen Konular:

1.Gün	Genel Network: Genel network yapısı, çalışma sistemi ve ekosistemi
2.Gün	Linux Sistem Sıkılaştırma: Linux sistemler hakkında genel bilgilendirme, Temel komut yapısı, İşletim sistemi genel çalışma yapısı, Çeşitli sıkılaştırma metotları (Crontab ve systemd)
3.Gün	SOC hizmetleri genel bilgilendirme: SOC kavramı, ekipleri, görevlendirme,ekosistem ve genel çalışma prensipleri(WAF,IDS/IPS,SIEM SOAR,EDR,DLP), Cyber Kill Chain, Mittre Att&ck
4.Gün	Wazuh: Wazuh nedir, kurulum aşamaları, çalışma sistemi,mimarisi,agent ekleme,basit düzeyde log yakalama(FIM dosya hareketlerinin loglanması)
5.Gün	CTI: Siber tehdit istihbaratı genel bilgilendirme,çalışma sistemi,Siber tehdit türleri,cyber kill chain,deepweb,darkweb,genel cti tool kullanımı örnekleri,Tor ağı

Altay Takımı Genel Süreç İşleyiş Programı

1.Hafta	Takım kabul maillerinin iletilmesi ve takımın kurulması (5 Eylül)
2.Hafta	Tanışma toplantısı yapılması ve genel süreç hakkında bilgilendirme (10 Eylül) Linux Sistem sıkılaştırma sunumu (13 Eylül)
3.Hafta	CTI sunumu(19 Eylül)
4.Hafta	Wazuh Ödev sunumu ve Red Team Sunumu (27 Eylül)
5.Hafta	OWASP Top – 10 Web Zafiyetleri Sunumu (4 Ekim)
6.Hafta	Windows Sistem Sıkılaştırma sunumu ve Persistence Sunumu (11 Ekim)
7.Hafta	Persistence sunumu , Firewall sunumu (19 Ekim)
8.Hafta	OpenCTI sunumu ve Wireshark sunumu (25 Ekim)
9.Hafta	Tatil (28-3 Kasım)
10.Hafta	Tatil (4-10 Kasım)
11.Hafta	Tatil (11-17 Kasım)
12.Hafta	FTK ve Autopsy sunumu (23 Kasım)
13.Hafta	Kape ve Windows Artifactlari sunumu, YARA Kuralı sunumu, Wazuh ve YARA Kullanarak Malware Tespiti (30 Kasım)
14.Hafta	Sunum Yok (7 Aralık)
15.Hafta	Snort IDS/IPS (14 Aralık)
16.Hafta	Zonguldak Eğitimi (16-22 Aralık)
17.Hafta	Zonguldak Eğitimi (23-29 Aralık) Genel Toplantı (29 Aralık)
18.Hafta	IOT Güvenliği (4 Ocak)
19.Hafta	OpenVAS sunumu (11 Ocak) - Adli Bilişim sunumları (12 Ocak)
20.Hafta	Tatil (13-19 Ocak)
21.Hafta	Genel network ve Wireshark sunumu(25 Ocak)

Eğitim İçeriği Tablosu

L0 Seviye Sunum İçerikleri

Sunum Seviyesi		Sunum İçeriği
1	L0	SIEM Nedir?
2	L0	EDR Nedir?
3	L0	IDS Nedir?
4	L0	IPS Nedir?
5	L0	Firewall 101
6	L0	SNORT
7	L0	Log Analizi (Graylog ve Wazuh Dahil)
8	L0	Honeypot
9	L0	OpenCTI ve Siber Tehdit İstihbaratı
10	L0	Blockchain'de Siber İstihbarat
11	L0	Frida ile Uygulama Hooklamak
12	L0	Software Cracking
13	L0	Kriptografi

L1 Seviye Sunum İçerikleri

Sunum Seviyesi		Sunum İçeriği
1	L1	Windows Sıkılaştırma
2	L1	Yetki Yükseltme ve Wazuh ile tespiti
3	L1	Pass the Hash Saldırısı ve Tespiti
4	L1	Atomic Red Team Log Analizi
5	L1	Active Directory
6	L1	Triage VM
7	L1	Regex
8	L1	Wireshark 101

L2 Seviye Sunum İçerikleri

Sunum Seviyesi		Sunum İçeriği
1	L2	Yara Kuralı ve Kullanımı (Wazuh ile Entegre)
2	L2	Zararlı Dosya Analizi
3	L2	Wazuh ve YARA ile Malware Tespiti
4	L2	OpenVAS ve Zafiyet Yönetimi
5	L2	FTK ve Autopsy ile Dijital Adli Analiz
6	L2	Pack ve Unpack
7	L2	Image File Execution Option Injection
8	L2	Volality Framework
9	L2	Suricata IDS/IPS
10	L2	API Security
11	L2	Sysmon
12	L2	Zero Trust Architecture
13	L2	Nessus
14	L2	Fail2Ban with Wazuh
15	L2	IO Port Restriction
16	L2	Cloud Security
17	L2	OpenEDR

Sunum İçerikleri Tablosu

Sunum Seviyesi: L0	**Sunum İçeriği: SIEM Nedir? (Tercihen Wazuh SIEM)**
Sunum İçeriği:SIEM hakkında teorik bilgi olmalı nedir ne işe yarar. Avantajlar/Dezavantajlar SOC ile ilişkisi. Temel işlevlerinden bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Sektörde yaygın olarak kullanılan SIEM ürünlerine örnekler verilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log nedir bilinmeli. Giriş seviyesi log analizi yapabilmeli. Basit düzeyde kural&korelasyon mantığı bilinmeli.	
Nasıl bir demo sunumu yapılabilir: SIEM genel ürün gösterimi, yapılandırılması ve kural yazımı. Tercihen Wazuh SIEM üzerinde log analizi ve saldırı tespiti	
Tavsiye ödev senaryosu: Tercihen Wazuh üzerinden log analizi raporu hazırlama veya saldırı senaryoları ile atak tespit etme raporlama	

Sunum Seviyesi: L0	**Sunum İçeriği: EDR Nedir?**
Sunum İçeriği:EDR hakkında teorik bilgi olmalı nedir ne işe yarar. Avantajlar/Dezavantajlar SOC ile ilişkisi Temel işlevlerinden bahsedilmeli SIEM'den farkı bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Sektörde yaygın olarak kullanılan EDR ürünlerine örnekler verilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log nedir bilinmeli. Giriş seviyesi log analizi yapabilmeli. Basit düzeyde kural&korelasyon mantığı bilinmeli. EDR genel mimarisi bilinmeli. Threat Hunting süreçlerine hakim olunmalı. Incident Response süreçlerine hakim olunmalı.	
Nasıl bir demo sunumu yapılabilir:EDR genel ürün gösterimi, yapılandırılması ve kural yazımı. EDR ürününün test olarak oluşturulmuş malware dosyasını tespiti	
Tavsiye ödev senaryosun: Şüpheli dosya işlemleri oluşturma ve bunların tespit edilerek raporlanması	

Sunum Seviyesi: L0	**Sunum İçeriği: IDS Nedir? (Tercihen Snort)**
Sunum İçeriği:IDS hakkında teorik bilgi olmalı nedir ne işe yarar. Avantajlar/Dezavantajlar SOC ile ilişkisi Temel işlevlerinden bahsedilmeli IPS ile farklarından ve entegrasyonundan kısaca bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı IDS çeşitlerinden bahsedilmeli (NIDS/HIDS) Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Sektörde yaygın olarak kullanılan IDS ürünlerine örnekler verilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli:İmza tabanlı ve anomali tabanlı algılama farkı bilinmeli. Genel hatları ile IDS mimarisi ve çalışma yapısı bilinmeli. Orta düzeyde kural&korelasyon mantığı bilinmeli.	
Nasıl bir demo sunumu yapılabilir:IDS genel ürün gösterimi, yapılandırılması ve kural yazımı. Tercihen Snort üzerinden Nmap simülesi ve tespit edilmesi	
Tavsiye ödev senaryosun: Şüpheli dosya işlemleri oluşturma ve bunların tespit edilerek raporlanması	

Sunum Seviyesi: L0	Sunum İçeriği: IPS Nedir?(Tercihen Snort)
Sunum İçeriği:IPS hakkında teorik bilgi olmalı nedir ne işe yarar. Avantajlar/Dezavantajlar SOC ile ilişkisi Temel işlevlerinden bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı IPS çeşitlerinden bahsedilmeli (NIPS/HIPS) IDS ile entegrasyonundan detaylı bahsedilmeli Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Sektörde yaygın olarak kullanılan IPS ürünlerine örnekler verilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel hatları ile IPS mimarisi ve çalışma yapısı bilinmeli. CTI süreçlerine entegrasyonu ve uygulaması bilinmeli. Orta düzeyde kural&korelasyon mantığı bilinmeli.	
Nasıl bir demo sunumu yapılabilir:IPS genel ürün gösterimi, yapılandırılması ve kural yazımı. SSH üzerinden brute force saldırısı ve tespit edilmesi	
Tavsiye ödev senaryosun: SMB üzerinden brute force ve bunların tespit edilerek raporlanması	
Tavsiye:IDS ve IPS konuları birbirleri ile doğrudan ilişkilidir. Bu sebeple beraber anlatılması daha kalıcı öğrenmeyi sağlayacaktır. Tercihen Snort üzerinden bu konular anlatılması tavsiye edilir.	

Sunum Seviyesi: L0	Sunum İçeriği: Firewall Nedir? (Tercihen UFW ve Iptables)
Sunum İçeriği: Firewall hakkında teorik bilgi olmalı nedir ne işe yarar. SOC için öneminden bahsedilmeli Temel işlevlerinden bahsedilmeli. Firewall çeşitlerinden bahsedilmeli. Avantaj ve dezavantajlarından bahsedilmeli Firewall politikalarından bahsedilmeli. Firewall üzerinden logların incelenmesinden bahsedilmeli. Firewall kural ekleme, trafik engelleme, ip engelleme gibi özellikleri gösterilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Sektörde yaygın olarak kullanılan Firewall ürünlerine örnekler verilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli : Genel network bilgisi. Log analizi yapabilmeli. Orta düzeyde kural&korelasyon mantığı bilinmeli.	
Nasıl bir demo sunumu yapılabilir: Firewall genel ürün gösterimi, yapılandırılması ve kural yazımı. Tercihen UFW üzerinden SSH erişim saldırısı ve bu saldırının engellenmesi.	
Tavsiye ödev senaryosu: Tercihen UFW üzerinden sadece HTTP/HTTPS isteklerini kabul eden ancak diğer isteklerin Firewall'a takılması için gerekli yapılandırılmaların yapılması ve raporlanması.	

Sunum Seviyesi: L0	Sunum İçeriği: Snort Nedir?
Sunum İçeriği: Snort hakkında teorik bilgi olmalı nedir ne işe yarar. Avantajlar/Dezavantajlar SOC ile ilişkisi. Temel işlevlerinden bahsedilmeli. Modlarından bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kural yapısı anlatılmalı ve örneklendirilmeli. Gerekli araçlarlar anlatılmalı. IDS ve IPS yapıları anlatılmalı. Örnek demo senaryoları ile sunum desteklenmeli. Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli : IDS/IPS çalışma mimarisi bilinmeli. Orta düzeyde kural&korelasyon mantığı bilinmeli. Log analizi yapabilme ve güvenlik politikaları hakkında bilgi sahibi olunmalı.	
Nasıl bir demo sunumu yapılabilir: Snort genel ürün gösterimi, yapılandırılması ve kural yazımı. SSH üzerinden brute force saldırısı tespiti ve loglanması IDS/IPS yapıları üzerinden gösterilmesi	
Tavsiye ödev senaryosu: Nmap tespiti ve raporlanması	

Sunum Seviyesi: L0	Sunum İçeriği: Log Analizi (Graylog ve Wazuh Dahil)
Sunum İçeriği: Log nedir Log türleri nelerdir.Log yönetimi ve analiz süreçleri detaylı olarak anlatılmalı Genel yapısı anlatılmalı.Analizi nasıl yapılmalı nelere dikkat edilmeli gibi konular derinlemesine anlatılmalı. Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli. SOC ile ilişkisinden bahsedilmeli. Genel hatları ile Graylog ve Wazuh anlatılmalı çalışma yapılarından bahsedilmeli. Graylog ve Wazuh kurulum süreçlerinden bahsedilmeli Graylog ve Wazuh üzerinden Log analiz süreci örnek demo senaryoları ile anlatılmalı. Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Giriş seviyesi log analizi yapabilmeli. Basit düzeyde kural&korelasyon mantığı bilinmeli. Wazuh ve Graylog ürünlerine genel olarak hakim olunmalı.	
Nasıl bir demo sunumu yapılabilir: Graylog ve Wazuh genel ürün gösterimi, yapılandırılması ve kural yazımı. Nmap tespiti, SSH brute force saldırısı ve loglarının incelenmesi	
Tavsiye ödev senaryosu: FTP üzerinden yetkisi dosya transferi tespiti ve raporlanması	

Sunum Seviyesi: L0	Sunum İçeriği:Honeypot
Sunum İçeriği: Honeypot nedir Türleri nelerdir anlatılamlı. SOC ile ilişkisinden bahsedilmeli Temel işlevlerinden bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Honeypot kurulum araç ve çözümlerinden bahsedilmel (Açık kaynaklı ve kurumsal) Örnek demo senaryoları ile sunum desteklenmeli. Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel network bilgisi. Honeypot yapısı. Saldırı türleri.	
Nasıl bir demo sunumu yapılabilir: SSH honeypot kurulması ve saldırgan ip adreslerinin tespiti	
Tavsiye ödev senaryosu: Nmap port taraması tespiti ve raporlanması	

Sunum Seviyesi: L0	Sunum İçeriği:OpenCTI ve Siber Tehdit İstihbaratı
Sunum İçeriği: Detaylı CTI nedir SOC için önemi nedir anlatılmalı TTP, APT grupları, Deep/Dark Web gibi konulardan anlatılmalı CTI çeşitleri ve süreçleri anlatılmalı OpenCTI platformu anlatılmalı SOC için önemi örnek senaryolar ile açıklanmalı(Bu platformu bir SOC analisti nasıl etkili kullanabilir) Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel CTI bilgisi. SOC için CTI süreçleri ve önemi bilinmeli	
Nasıl bir demo sunumu yapılabilir: OpenCTI genel ürün gösterimi, yapılandırılması.	
Tavsiye ödev senaryosu: OpenCTI üzerinden çeşitli APT grupları incelenmesi ve raporlanması	

Sunum Seviyesi: L0	Sunum İçeriği:Blockchain'de Siber İstihbarat
Sunum İçeriği: Blockchain nedir CTI ile ilişkisi detaylı olarak anlatılmalı Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli SOC ile ilişkisi anlatılmalı Blockchain ve MITRE ATT&CK Framework ilişkisi, TTP'lerin analizindan bahsedilmeli Blockchain ve Siber Tehdit araçlarına örnekler verilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel CTI bilgisi. SOC için CTI süreçleri ve önemi bilinmeli	
Nasıl bir demo sunumu yapılabilir: -	
Tavsiye ödev senaryosu: -	

Sunum Seviyesi: L0	Sunum İçeriği: Frida ile uygulama hooklamak
Sunum İçeriği: Frida hakkında teorik bilgi olmalı nedir ne işe yarar. Temel işlevlerinden bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Frida ile uygulama hooklamaya karşı alınabilecek askiyonlardan bahsedilmeli SOC ile ilişkisinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Yazılım bilgisi. Tersine mühendislik yöntemleri. Mobil uygulama güvenliği.	
Nasıl bir demo sunumu yapılabilir: Frida genel ürün gösterimi, yapılandırılması Şifrelenmiş bir değerin hooklama yoluyla düz metin olarak elde edilmesi	
Tavsiye ödev senaryosu: Gönderilen veya alınan verilerin Frida ile değiştirilmesi ve raporlanması	

Sunum Seviyesi: L0	Sunum İçeriği: Software Cracking
Sunum İçeriği: Software Cracking nedir anlatılmalı Temel işlevlerinden bahsedilmeli. Software Cracking türleri ve teknikleri detaylı olarak anlatılmalı Tersine mühendislik süreçleri anlatılmalı İş akışından bahsedilmeli Cracking araç ve yazılımları anlatılmalı Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Software Cracking karşı alınabilecek askiyonlardan bahsedilmeli SOC ile ilişkisinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Yazılım bilgisi. Orta seviye tersine mühendislik.	
Nasıl bir demo sunumu yapılabilir: Winrar cracking	
Tavsiye ödev senaryosu: Crackmes sitesinden basit seviyede uygulamaların çözülmesi ve raporlanması	

Sunum Seviyesi: L0	Sunum İçeriği: Kriptografi
Sunum İçeriği: Kriptografi nedir ne işe yarar detaylıca anlatılmalı Temel işlevlerinden bahsedilmeli. SOC için öneminde bahsedilmeli Kriptografi çeşitleri anlatılmalı aralarındaki farklardan bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel Kriptografi bilgisi	
Nasıl bir demo sunumu yapılabilir:Çeşitli şifreleme algoritmaları ile şifreleme ve şifre çözme	
Tavsiye ödev senaryosu: En çok kullanılan şifreleme algoritmaların raporlanması	

Sunum Seviyesi: L1	Sunum İçeriği: Windows Sıkılaştırma
Sunum İçeriği: Windows OS detaylıca anlatılmalı çalışma prensipleri mimarisi anlatılmalı Sıkılaştırmanın SOC için önemi anlatılmalı Sıkılaştırma iş akışı anlatılmalı Kullanıcı hesapları ve yetkilendirme, Yama yönetimi ve güncellemeler, Ağ güvenliği, Loglama ve izleme, GPO ile güvenlik politikaları vb. Alanlarda sıkılaştırma derinlemesine anlatılmalı Örnek uygulama ve demo senaryolar gösterilmeli Sıkılaştırma araçlarından bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Orta seviye Windows OS, Windows güvenlik açıklarının teknik analizi	
Nasıl bir demo sunumu yapılabilir: Windows OS üzerinden çeşitli zafiyetler oluşturma ve bu zafiyetlere karşı sıkılaştırma teknikleri, Sıkılaştırma araçlar gösterimi (Tercihen HardeningKitty)	
Tavsiye ödev senaryosu: Windwos OS üzerinde çeşitli sıkılaştırmalar yapılması ve raporlanması	

Sunum Seviyesi: L1	Sunum İçeriği: Yetki yükseltme ve Wazuh ile tespiti
Sunum İçeriği: Yetki yükseltme yöntemlerinden bahsedilmeli SOC için önemi anlatılmalı Yetki yükseltme teknikleri detaylıca anlatılmalı Yetki yükseltme örnek senaryolar ile anlatılmalı Wazuh SIEM kullanarak tespit edilmeli Log analizi detaylıca anlatılmalı Örneklerde kullanılan saldırıların teknik ve taktikleri MITRE ATT&CK Framework üzerinden eşleştirilmeli Yetki yükseltme saldırısına karşı alınabilecek önlemler ve aksiyonlardan bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Orta seviyesi log analizi yapabilmeli. Orta düzeyde kural&korelasyon mantığı bilinmeli. Orta seviye Wazuh SIEM bilinmeli. Yetki yükseltme saldırıları hakkında bilgi sahibi olunmalı	
Nasıl bir demo sunumu yapılabilir: Yetki yükseltme saldırı senaryosu ve Wazuh ile tespiti	
Tavsiye ödev senaryosu: Yetki yükseltme saldırı senaryosu ve Wazuh ile tespiti raporlanması	

Sunum Seviyesi: L1	Sunum İçeriği: Pass the Hash Saldırısı ve Tespiti
Sunum İçeriği: Pass the Hash saldırısı anlatılmalı Saldırının çalışma mekanizması anlatılmalı İş akışı gösterilmeli SOC için öneminden bahsedilmeli PtH saldırsı tespit yöntemlerinden bahsedilmeli Örnek demo senaryolar gösterilmeli Örneklerde kullanılan saldırıların teknik ve taktikleri MITRE ATT&CK Framework üzerinden eşleştirilmeli PtH saldırısına karşı alınabilecek önlemler ve aksiyonlardan bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: PtH saldırı vektörü hakkında genel bilgi	
Nasıl bir demo sunumu yapılabilir: PtH saldırı senaryosu ve tespiti	
Tavsiye ödev senaryosu: PtH saldırı senaryosu ve tespiti raporlanması	

Sunum Seviyesi: L1	Sunum İçeriği:Atomic Red Team Log Analizi
Sunum İçeriği:ART hakkında teorik bilgi olmalı nedir ne işe yarar. Avantajlar/Dezavantajlar SOC ile ilişkisi. Temel işlevlerinden bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Örnek demo senaryolar gösterilmeli Örneklerde kullanılan saldırıların teknik ve taktikleri MITRE ATT&CK Framework üzerinden eşleştirilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Orta seviyesi log analizi yapabilmeli. İyi seviyede MITRE ATT&CK Framework bilinmeli.	
Nasıl bir demo sunumu yapılabilir: ART genel ürün gösterimi, yapılandırılması. UAC bypass tespiti log analizi.	
Tavsiye ödev senaryosu: Powershell kötüye kullanımı tespiti ve raporlanması	

Sunum Seviyesi: L1	Sunum İçeriği: Active Directory
Sunum İçeriği:AD hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Temel işlevlerinden bahsedilmeli. Bileşenleri anlatılmalı Grup politikaları anlatılmalı. AD ile ilgili tehditler ve güvenliği anlatılmalı Örnek demo senaryolar gösterilmeli Örneklerde kullanılan saldırıların teknik ve taktikleri MITRE ATT&CK Framework üzerinden eşleştirilmeli AD sıkılaştırma anlatılmalı Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Orta seviye Windows OS	
Nasıl bir demo sunumu yapılabilir: AD kurulum ve yapılandırılması. Tehdit simülasyonu ve bu tehditlere karşı sıkılaştırma yöntemleri	
Tavsiye ödev senaryosu:AD kurulum ve yapılandırılması raporu	

Sunum Seviyesi: L1	Sunum İçeriği: Triage VM
Sunum İçeriği: Triage hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Kullanım alanlarından bahsedilmeli Temel işlevlerinden bahsedilmeli. Bileşenleri anlatılmalı Triage VM'de kullanılan temel araçlar anlatılmalı Örnek demo senaryolar gösterilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi. Adli bilişim süreçleri hakkında genel bilgi.	
Nasıl bir demo sunumu yapılabilir: Triage VM kurulum ve yapılandırılması. Bellek analizi,Log analizi,Zararlı yazılım analizi, Ağ trafiği analizi	
Tavsiye ödev senaryosu: Bellek analizi,Log analizi,Zararlı yazılım analizi, Ağ trafiği analizi raporlanması	

Sunum Seviyesi: L1	Sunum İçeriği: Regex
Sunum İçeriği: Regex hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Kullanım alanlarından bahsedilmeli Regex temellerinden bahsedilmeli Karakter sınıflarından bahsedilmeli Temel işlevlerinden bahsedilmeli. Bileşenleri anlatılmalı Örnek demo senaryolar gösterilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi. Regex hakkında genel bilgi	
Nasıl bir demo sunumu yapılabilir: Gerçek bir log dosyasından belirli bir olay türünü çıkarma	
Tavsiye ödev senaryosu: Çeşitli regex örnekleri ve raporlanması	

Sunum Seviyesi: L1	Sunum İçeriği: Wireshark
Sunum İçeriği: Wireshark hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Kullanım alanlarından bahsedilmeli Temel işlevlerinden bahsedilmeli. Filtreleri anlatılmalı Ağ analizi yaparken nelere dikkat edilmesi gerektiği anlatılmalı Örnek demo senaryolar gösterilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi. Genel network bilgisi	
Nasıl bir demo sunumu yapılabilir: DDoS saldırı tespiti ve paket analizi	
Tavsiye ödev senaryosu: HTTP,DNS,TCP/IP,UDP protokollerinin trafiği incelenmesi, filtre kullanımı ve raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: YARA Kuralı ve Kullanımı (Wazuh ile Malware Tespiti)
Sunum İçeriği: YARA motoru hakkında teorik bilgi olmalı nedir ne işe yarar. Kullanım alanlarından bahsedilmeli Temel işlevlerinden bahsedilmeli. YARA kural yapısı detaylı olarak anlatılmalı Wazuz SIEM ile entegrasyonu anlatılmalı. Gerekli yapılandırılmalar gösterilmeli Wazuh SIEM kullanarak örnek demo senaryolar gösterilmeli Wazuh SIEM kullanarak zararlı yazılım tespit tekniklerinin anlatılması ve gösterilmesi Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi. Orta seviye Wazuh bilgisi. Orta düzeyde kural&korelasyon mantığı bilinmeli.	
Nasıl bir demo sunumu yapılabilir: YARA kullanarak zararlı tespiti Wazuh üzerinden gösterilmesi	
Tavsiye ödev senaryosu: Çeşitli YARA kural örnekleri raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: Zararlı Dosya Analizi
Sunum İçeriği: Zararlı dosya analiz süreçleri anlatılmalı Temel işlevlerinden bahsedilmeli. Zararlı dosya türleri ve teknikleri detaylı olarak anlatılmalı Tersine mühendislik süreçleri anlatılmalı İş akışından bahsedilmeli Zararlı dosya analizi için araç ve yazılımları anlatılmalı Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Örnek demo senaryolar gösterilmeli SOC ile ilişkisinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Orta seviye tersine mühendislik	
Nasıl bir demo sunumu yapılabilir: Zararlı dosya tespiti ve analizi (Tercihen Wannacry)	
Tavsiye ödev senaryosu: Basit düzeyde zararlı dosya analizi	

Sunum Seviyesi: L2	Sunum İçeriği: OpenVAS ve Zafiyet Yönetimi
Sunum İçeriği: OpenVAS nedir ne işe yarar anlatılmalı Temel işlevlerinden bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Zafiyet yönetim süreçleri anlatılmalı Örnek demo senaryolar gösterilmeli SOC ile ilişkisinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel kırmızı takım bilgisi	
Nasıl bir demo sunumu yapılabilir: OpenVAS genel ürün gösterimi, yapılandırılması. Zafiyetli bir makinenin zafiyet taraması ve zafiyetlerin tespiti	
Tavsiye ödev senaryosu: Zafiyetli bir makinenin zafiyet taraması ve zafiyetlerin tespiti raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: FTK ve Autopsy ile Dijital Adli Analiz
Sunum İçeriği:FTK ve Autopsy hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Kullanım alanlarından bahsedilmeli Adli bilişi süreçleri anlatılmalı İş akış süreçleri anlatılmalı Temel işlevlerinden bahsedilmeli. Bileşenleri anlatılmalı Örnek demo senaryolar gösterilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi. Adli bilişim süreçleri hakkında genel bilgi.	
Nasıl bir demo sunumu yapılabilir: FTK ve Autopsy kurulum ve temel yapılandırılmaları Disk imaj analizi	
Tavsiye ödev senaryosu: FTK ve Autopsy hakkında genel rapor	

Sunum Seviyesi: L2	Sunum İçeriği: Pack ve Unpack
Sunum İçeriği: Pack ve Unpack hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Kullanım alanlarından bahsedilmeli Temel işlevlerinden bahsedilmeli. Bileşenleri anlatılmalı Örnek demo senaryolar gösterilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel network bilgisi	
Nasıl bir demo sunumu yapılabilir: -	
Tavsiye ödev senaryosu: -	

Sunum Seviyesi: L2	Sunum İçeriği: Image File Execution Option Injection
Sunum İçeriği:IFEO hakkında teorik bilgi olmalı nedir ne işe yarar. Teknik detayları anlatılmalı. İş akışı anlatılmalı SOC ile ilişkisi anlatılmalı Kullanım senaryoları ve taktikleri anlatılmalı IFEO Injection teknikleri ve korunma yöntemleri anlatılmalı IFEO Injection tespit yöntemleri anlatılmalı Örnek demo senaryolar gösterilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel Windows OS bilgisi. IFEO Injection hakkında genel bilgi	
Nasıl bir demo sunumu yapılabilir: IFEO Injection saldırısı ve tespiti	
Tavsiye ödev senaryosu: IFEO Injection saldırısı ve tespiti ve raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: Image File Execution Option Injection
Sunum İçeriği:IFEO hakkında teorik bilgi olmalı nedir ne işe yarar. Teknik detayları anlatılmalı. İş akışı anlatılmalı SOC ile ilişkisi anlatılmalı Kullanım senaryoları ve taktikleri anlatılmalı IFEO Injection teknikleri ve korunma yöntemleri anlatılmalı IFEO Injection tespit yöntemleri anlatılmalı Örnek demo senaryolar gösterilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel Windows OS bilgisi. IFEO Injection hakkında genel bilgi	
Nasıl bir demo sunumu yapılabilir: IFEO Injection saldırısı ve tespiti	
Tavsiye ödev senaryosu: IFEO Injection saldırısı ve tespiti ve raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: Volality Framework
Sunum İçeriği: Volality Framework hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Kullanım alanlarından bahsedilmeli Adli bilişi süreçleri anlatılmalı İş akış süreçleri anlatılmalı Temel işlevlerinden bahsedilmeli. Bileşenleri anlatılmalı Örnek demo senaryolar gösterilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Adli bilişim süreçleri hakkında genel bilgi. Volality Framework hakkında genel bilgi	
Nasıl bir demo sunumu yapılabilir: Volality Framework kurulum ve temel yapılandırılmaları Proses Analizi,Ağ analizi,Zararlı Yazılım analizi	
Tavsiye ödev senaryosu: FTK ve Autopsy hakkında genel rapor	

Sunum Seviyesi: L2	Sunum İçeriği: Suricata Nedir?
Sunum İçeriği: Suricata hakkında teorik bilgi olmalı nedir ne işe yarar. Avantajlar/Dezavantajlar SOC ile ilişkisi. Temel işlevlerinden bahsedilmeli. Modlarından bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kural yapısı anlatılmalı ve örneklendirilmeli. Gerekli araçlarlar anlatılmalı. IDS ve IPS yapıları anlatılmalı. Örnek demo senaryoları ile sunum desteklenmeli. Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli : IDS/IPS çalışma mimarisi bilinmeli. Orta düzeyde kural&korelasyon mantığı bilinmeli. Log analizi yapabilme ve güvenlik politikaları hakkında bilgi sahibi olunmalı.	
Nasıl bir demo sunumu yapılabilir: Suricata genel ürün gösterimi, yapılandırılması ve kural yazımı. SSH üzerinden brute force saldırısı tespiti ve loglanması IDS/IPS yapıları üzerinden gösterilmesi	
Tavsiye ödev senaryosu: Nmap tespiti ve raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: API Security
Sunum İçeriği:API security hakkında teorik bilgi olmalı nedir ne işe yarar.SOC ile ilişkisi. API security güvenlik tehditleri API security zafiyetleri anlatılmalı API security zafiyetlerine karşı alınabilecek önlemlerden bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Örnek demo senaryolar gösterilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli : Network bilgisi ve güvenliği hakkında bilgi sahibi olunmalı. Yazılım bilgisi API hakkında bilgi sahibi olunmalı	
Nasıl bir demo sunumu yapılabilir: Basit bir API üzerinde güvenlik testleri ve zafiyetleri tespiti	
Tavsiye ödev senaryosu: Basit bir API üzerinde güvenlik testleri ve zafiyetleri tespiti raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: Sysmon
Sunum İçeriği: Sysmon hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi anlatılmalı Kullanım alanlarından bahsedilmeli Sistem olayları nasıl kaydedilir nasıl yönetilir nasıl analiz edilir anlatılmalı Temel işlevlerinden bahsedilmeli. Saldırı tespiti nasıl yapılır anlatılmalı. Sysmon kullanarak analiz süreçlerinden bahsedilmeli Örnek demo senaryolar gösterilmeli Wazuh SIEM entegrasyonu anlatılmalı Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi. Genel network bilgisi. Genel Wazuh SIEM bilgisi. Sistem olayları nasıl kaydedildiği ve nasıl analiz edildiği bilinmeli. Genel Windows OS bilgisi	
Nasıl bir demo sunumu yapılabilir: Sysmon kurulum ve yapılandırma ayarları. Şüpheli dosya hareketlerinin tespit edilmesi ve analizi	
Tavsiye ödev senaryosu: Basit düzeyde zararlı yazılım tespiti analizi ve raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: Zero Trust Architecture
Sunum İçeriği:ZTA nedir ne işe yarar detaylıca anlatılmalı Temel işlevlerinden bahsedilmeli. SOC için öneminde bahsedilmeli Temel bileşenlerinden bahsedilmeli ZTA mimarisin uygulama alanlarından ve kullanım örneklerinden bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Klasik mimarilerinden farkları anlatılmalı Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel ZTA hakkında bilgi sahibi olunmalı	
Nasıl bir demo sunumu yapılabilir:-	
Tavsiye ödev senaryosu:-	

Sunum Seviyesi: L2	Sunum İçeriği: Nessus
Sunum İçeriği: Nessus nedir ne işe yarar anlatılmalı Temel işlevlerinden bahsedilmeli. Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Zafiyet yönetim süreçleri anlatılmalı Örnek demo senaryolar gösterilmeli SOC ile ilişkisinden bahsedilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel kırmızı takım bilgisi	
Nasıl bir demo sunumu yapılabilir: Nessus genel ürün gösterimi, yapılandırılması. Zafiyetli bir makinenin zafiyet taraması ve zafiyetlerin tespiti	
Tavsiye ödev senaryosu: Zafiyetli bir makinenin zafiyet taraması ve zafiyetlerin tespiti raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: Fail2Ban with Wazuh
Sunum İçeriği: Fail2Ban hakkında teorik bilgi olmalı nedir ne işe yarar. Kullanım alanlarından bahsedilmeli Temel işlevlerinden bahsedilmeli. SOC için öneminden bahsedilmeli Wazuz SIEM ile entegrasyonu anlatılmalı. Gerekli yapılandırılmalar gösterilmeli Wazuh SIEM kullanarak örnek demo senaryolar gösterilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi. Orta seviye Wazuh bilgisi. Orta düzeyde kural&korelasyon mantığı bilinmeli.	
Nasıl bir demo sunumu yapılabilir:SSH brute force saldırı tespiti ve engellenmesi	
Tavsiye ödev senaryosu: SMB brute force saldırı tespiti engellenmesi ve raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: IO Port Restriction
Sunum İçeriği:IO Port Restriction nedir ne işe yarar detaylıca anlatılmalı Temel işlevlerinden bahsedilmeli. SOC için öneminde bahsedilmeli IO Port Restriction uygulama alanlarından ve kullanım örneklerinden bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Windows ve Linux üzerinden örnek senaryolar ile gösterilmeli Wazuh SIEM ile örnekler verilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Genel sistem bilgisi. Log analizi. Orta seviye Wazuh bilgisi. Orta düzeyde kural&korelasyon mantığı bilinmeli.	
Nasıl bir demo sunumu yapılabilir: Şüpheli IO port hareketlerinin tespiti ve analizi	
Tavsiye ödev senaryosu: Şüpheli IO port hareketlerinin tespiti ve analizi raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: Cloud Security
Sunum İçeriği: Cloud security hakkında teorik bilgi olmalı nedir ne işe yarar.SOC ile ilişkisi. Cloud security güvenlik tehditleri Cloud security zafiyetleri anlatılmalı Cloud security zafiyetlerine karşı alınabilecek önlemlerden bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Örnek demo senaryolar gösterilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli : Network bilgisi ve güvenliği hakkında bilgi sahibi olunmalı. Bulut bilişim hakkında genel bilgi sahibi olunmalı	
Nasıl bir demo sunumu yapılabilir: Basit bir API üzerinde güvenlik testleri ve zafiyetleri tespiti	
Tavsiye ödev senaryosu: Basit bir API üzerinde güvenlik testleri ve zafiyetleri tespiti raporlanması	

Sunum Seviyesi: L2	Sunum İçeriği: OpenEDR Nedir?
Sunum İçeriği: OpenEDR hakkında teorik bilgi olmalı nedir ne işe yarar. SOC ile ilişkisi Temel işlevlerinden bahsedilmeli Çalışma prensipleri anlatılmalı, mimarisi genel hatları ile anlatılmalı Kullanım alanlarından ve kullanım örneklerinden bahsedilmeli Örnek demo senaryolar gösterilmeli Kurulum süreçlerinden bahsedilmeli Kaynaklar ve makaleler içermeli	
Bu sunum için neler bilinmeli: Log analizi yapabilmeli. Basit düzeyde kural&korelasyon mantığı bilinmeli. EDR genel mimarisi bilinmeli. Threat Hunting süreçlerine hakim olunmalı. Incident Response süreçlerine hakim olunmalı.	
Nasıl bir demo sunumu yapılabilir:EDR genel ürün gösterimi, yapılandırılması ve kural yazımı. EDR ürününün test olarak oluşturulmuş malware dosyasını tespiti	
Tavsiye ödev senaryosu: Şüpheli dosya işlemleri oluşturma ve bunların tespit edilerek raporlanması	