DERS BİLGİ FORMU

<table>
<tr><td>DERSİN ADI</td><td colspan="4">SİBER OLAYLARA MÜDAHALE</td></tr>
<tr><td>DERSİN SINIFI</td><td colspan="4">11. Sınıf</td></tr>
<tr><td>DERSİN SÜRESİ</td><td colspan="4">Haftalık 4 Ders Saati</td></tr>
<tr><td>DERSİN AMACI</td><td colspan="4">Bu derste öğrenciye; siber olay yönetimi, siber olay izleme, siber olay log yönetimi ve siber olaylara müdahale uygulamaları gerçekleştirme ile ilgili bilgi ve becerilerin kazandırılması amaçlanmaktadır.</td></tr>
<tr><td>DERSİN ÖĞRENME KAZANIMLARI</td><td colspan="4">1. Siber olaylara müdahale için olay yönetimini açıklayarak Dünyada ve Türkiye’de siber olaylara müdahale ekip ve merkezlerini açıklar.
2. Olay izleme yöntemlerini açıklayarak olay izleme uygulaması yapar.
3. Siber olaylara müdahale için log yönetimini açıklayarak siber olaylara müdahale için log yönetim araçlarını kullanır.
4. Siber olaylara müdahale senaryoları hazırlayarak siber olay sonrası gerçekleştirilecek işlemleri uygular.</td></tr>
<tr><td>EĞİTİM ÖĞRETİM ORTAMI VE DONANIMI</td><td colspan="4">Ortam: Bilişim Teknolojileri Laboratuvarı

Donanım: Akıllı tahta/projeksiyon, bilgisayar, yazıcı/tarayıcı, ağ cihazları, sanallaştırılmış bilgisayar</td></tr>
<tr><td>ÖLÇME VE DEĞERLENDİRME</td><td colspan="4">Bu derste; öğrenci performansını belirlemeye yönelik çalışmalar değerlendirilirken gözlem formu, derecelendirme ölçeği, dereceli puanlama anahtarı gibi ölçme araçlarından uygun olanlar seçilerek kullanılabilir. Öz değerlendirme formu ile akran değerlendirme formu kullanılarak da öğrencilerin, öğretimin süreç boyutuna katılmaları sağlanabilir.</td></tr>
<tr><td rowspan="5">KAZANIM SAYISI VE SÜRE TABLOSU</td><td>ÖĞRENME BİRİMİ</td><td>KAZANIM SAYISI</td><td>DERS SAATİ</td><td>ORAN (%)</td></tr>
<tr><td>Siber Olay Yönetimi</td><td>2</td><td>24</td><td>17</td></tr>
<tr><td>Siber Olay İzleme</td><td>2</td><td>36</td><td>25</td></tr>
<tr><td>Siber Olay Log Yönetimi</td><td>2</td><td>40</td><td>28</td></tr>
<tr><td>Siber Olaylara Müdahale Uygulamaları</td><td>3</td><td>44</td><td>30</td></tr>
<tr><td colspan="2">TOPLAM</td><td>9</td><td>144</td><td>100</td></tr>
</table>

ÖĞRENME BİRİMİ	KONULAR	ÖĞRENME BİRİMİ KAZANIMLARI VE ÖĞRENME BİRİMİNDEKİ KAZANIMLARIN AÇIKLAMALARI
Siber Olay Yönetimi	• Siber Olay Yönetimi • Siber Olaylara Müdahale Ekipleri	**1. Siber olaylara müdahale için olay yönetimini açıklar.** • Siber olay yönetimi süreci açıklanır. • Siber olay genel terim ve kavramları [Siber güvenlik, bilgi güvenliliği, son kullanıcı güvenliği, zafiyet yönetimi, SOC, kimlik ve erişim yönetimi (IAM), maksimum önlem, minimum taviz izleme vb.] açıklanır. • Olay müdahale planının önemi açıklanır. • Olaylara müdahalede siber güvenliğin rolü açıklanır. • Olay müdahalesinin yedi aşaması (Hazırlık, Tanılama, Sınırlama, Yok Etme, İyileştirme, Öğrenilen Dersler, Devam Eden İyileştirme) açıklanır. • Olay müdahale çerçeveleri (NIST, SANS vb.) açıklanır. • Olası bir siber olaya karşı müdahale planı uygulaması gerçekleştirilir. **2. Dünyada ve Türkiye'de siber olaylara müdahale ekip ve merkezlerini açıklar.** • CERT (Computer Emergency Response Team) açıklanır. • CSIRT (Computer Security Incident Response Team) açıklanır. • ENISA (European Union Agency for Cybersecurity) açıklanır. • FIRST (Forum of Incident Response and Security Teams) açıklanır. • NCSC (National Cyber Security Centre) açıklanır. • USOM (Ulusal Siber Olaylara Müdahale Merkezi) açıklanır. • SOME (Siber Olaylara Müdahale Ekibi) açıklanır. • TÜBİTAK BİLGEM SGE (Siber Güvenlik Enstitüsü) açıklanır. • KVKK (Kişisel Verileri Koruma Kurumu) açıklanır. • EMEG (Enerji Sektörü SOME Grubu) açıklanır. • Türkiye Siber Güvenlik Kümelenmesi açıklanır.
Siber Olay İzleme	• Olay İzleme Yöntemleri • Olay İzleme Uygulaması	**1. Olay izleme yöntemlerini açıklar.** • Siber olay izleme politikaları (Öncelik Sıralaması, İzleme Kuralları ve Politikaları, Saldırı Senaryoları, Tehdit Sıralamaları vb.) açıklanır. • Siber olay izleme yöntem ve araçları [SIEM araçları, SOAR, Firewall, Endpoint Detection and Response (EDR) vb.] açıklanır. • Siber olay kapsamında izlenmesi gereken unsurlar (network logları vb.) nedenleri ile açıklanır. • Tehdit avcılığı (Threat Hunting) ve anomali tespiti açıklanır. **2. Olay izleme uygulaması yapar.** • Olay izleme aracı kurulumu (Wazuh vb.) uygulaması gerçekleştirilir. • Olay izleme uygulaması gerçekleştirilir.

Siber Olay Log Yönetimi	• Log Yönetimi • Log Yönetim Araçları	**1. Siber olaylara müdahale için log yönetimini açıklar.** • Log türleri [transection log (SQL server'a ait loglar), event log (Windows sisteminde tutulan loglar), syslog (Unix/Linux sistemlerde kullanılan loglar)] açıklanır. • Log içerik bilgileri açıklanır. • Web log kaynakları (Erişim logları, OS logları, log türleri, potansiyel tehditler, saldırı senaryoları, web server türleri, WAF logları vb.) açıklanır. • Network log kaynakları (Firewall, Switch, Router, VPN, Proxy, IPS'ye ait loglar vb.) açıklanır. • Veri tabanı logları (SQL logları, connection logları, kullanıcı logları vb.) açıklanır. • Endpoint logları [Antivirüs logları, host-based firewall logları, EDR logları, kullanıcı ve sistem hesap logları, Data Loss Prevention (DLP) logları vb.] açıklanır. **2. Siber olaylara müdahale için log yönetim araçlarını kullanır.** • Agent yöntemiyle loglama uygulaması gerçekleştirilir. • Log yönlendirme ile loglama uygulaması gerçekleştirilir. • API entegrasyon yöntemi ile loglama uygulaması gerçekleştirilir. • Windows sistemlerde sysmon kurulumu uygulaması gerçekleştirilir. • Windows sistemlerde sysmon config yapılandırması uygulaması gerçekleştirilir. • Sysmon ile oluşturulan logların SIEM araçlarıyla analizi uygulaması gerçekleştirilir. • Yerel güvenlik ilkelerinden logları aktif hâle getirme uygulaması gerçekleştirilir. • Linux sistemlerde log görüntüleme uygulaması gerçekleştirilir. • Linux üzerinde Agent kurularak loglama uygulaması gerçekleştirilir. • Logları ayrıştırma işlemi (Normalizasyon, Sınıflandırma, Korelasyon) uygulaması gerçekleştirilir. • Kullanıcı olaylarına göre korelasyon uygulaması gerçekleştirilir.
Siber Olaylara Müdahale Uygulamaları	• Siber Olaylara Müdahale Adımları • Olay Müdahale Senaryoları • Olay Sonrası Gerçekleştirilecek İşlemler	**1. Siber olaylara müdahale adımlarına ait uygulamaları yapar.** • Olay tespiti uygulaması gerçekleştirilir. • Olayın sınıflandırılması ve önceliklendirilmesi uygulaması gerçekleştirilir. Müdahale planının hazırlanması uygulaması gerçekleştirilir. **2. Olay müdahale senaryoları uygular.** • Web saldırılarına karşı müdahale uygulaması gerçekleştirilir. • Network saldırılarına karşı müdahale (DDoS vb.) uygulaması gerçekleştirilir. • Veri ihlaline karşı müdahale uygulaması gerçekleştirilir. • Malware saldırılarına karşı müdahale uygulaması gerçekleştirilir.

		3. Olay sonrası gerçekleştirilecek işlemleri uygular. • Olayın analizi ve inceleme raporu hazırlanması uygulaması gerçekleştirilir. • İyileştirme adımları uygulaması gerçekleştirilir. • Olaydan ders çıkarma ve güvenlik politikalarını düzenleme uygulaması gerçekleştirilir. • Kullanıcı ve yönetici bilgilendirmesi uygulaması gerçekleştirilir. • Saldırı takibi uygulaması gerçekleştirilir.

UYGULAMA FAALİYETLERİ/TEMRİNLER	
Uygulama faaliyeti/temrinler; ders kazanımına uygun olarak okulun fiziki kapasitesi ve donatımı, öğrenci sayısı göz önünde bulundurularak en fazla uygulama faaliyeti/temrini yaptıracak şekilde meslek, alan zümre öğretmenler kurulu tarafından seçilir. Meslek, alan zümre öğretmenleri tarafından aşağıda yer alan temrinlerden farklı temrinlerin uygulanmasına karar verilebilir.	
Siber Olay Yönetimi	**1.** Olay müdahale planının önemi açıklamak. **2.** Olası bir siber olaya karşı müdahale planı uygulaması yapmak. **3.** Dünyada ve Türkiye'de siber olaylara müdahale ekip ve merkezleri hakkında bilgi toplayarak sunmak.
Siber Olay İzleme	**1.** Olay izleme aracı kurulumu yapmak. **2.** Olay izleme uygulaması yapmak.
Siber Olay Log Yönetimi	**1.** Siber olaylara müdahale için log yönetimini yapmak. **2.** Agent yöntemiyle loglama uygulaması yapmak. **3.** Log yönlendirme ile loglama uygulaması yapmak. **4.** API entegrasyon yöntemi ile loglama uygulaması yapmak. **5.** Windows sistemlerde sysmon kurulumu uygulaması yapmak. **6.** Sysmon ile oluşturulan logların SIEM araçlarıyla analizi uygulaması yapmak. **7.** Linux üzerinde Agent kurularak loglama uygulaması yapmak. **8.** Logları ayrıştırma işlemi (Normalizasyon, Sınıflandırma, Korelasyon) uygulaması yapmak.
Siber Olaylara Müdahale Uygulamaları	**1.** Müdahale planının hazırlanması uygulaması yapmak. **2.** Web saldırılarına karşı müdahale uygulaması yapmak. **3.** Network saldırılarına karşı müdahale (DDoS vb.) uygulaması yapmak. **4.** Veri ihlaline karşı müdahale uygulaması yapmak. **5.** Malware saldırılarına karşı müdahale uygulaması yapmak. **6.** Olayın analizi ve inceleme raporu hazırlanması uygulaması yapmak. **7.** İyileştirme adımları uygulaması yapmak. **8.** Olaydan ders çıkarma ve güvenlik politikalarını düzenleme uygulaması yapmak. **9.** Kullanıcı ve yönetici bilgilendirmesi uygulaması yapmak. **10.** Saldırı takibi uygulaması yapmak.

DERSİN UYGULANMASINA İLİŞKİN AÇIKLAMALAR
1. Her öğrencinin uygulama yapabilmesi için uygun ortam oluşturulmalıdır. **2.** Uygulama faaliyetlerinde iş sağlığı ve güvenliğine ilişkin risk ve tehlike oluşturabilecek her türlü duruma karşı tedbirler alınmalıdır. **3.** Ders işlenirken öğrencilerde birlikte iş yapabilme, kendini ifade edebilme, sorumluluk bilinci, öz güven vb. değer, tutum ve davranışları ön plana çıkaran etkinliklere yer verilmelidir. Bu etkinliklerde beyin fırtınası, grup tartışması, düz anlatım, soru cevap, örnek olay incelemesi gibi yöntem ve teknikler kullanılabilir. **4.** Konu anlatımından ve örnek çalışmalardan sonra dersin öğrenme kazanımlarının öğrencide pekiştirilmesi amacıyla birden fazla uygulama faaliyeti yapılmalıdır.