Bölüm 3

Siber Güvenliğin Temelleri: Tehditler, Koruma Yöntemleri, Açık Kaynak Yazılımlar, Yapay Zekâ ve Trend Analizleri ile Güvenlik Uyum Yönetimi

Hüseyin Parmaksız[1]

Özet

Bu çalışmada siber güvenliğin temelleri, güncel tehditler, korunma yöntemleri, açık kaynak yazılımlar, yapay zekâ uygulamaları ve trend analizleri incelenmektedir. Keycloak, PacketFence, Wazuh, OPNsense, Coroza ve OpenCTI gibi açık kaynak araçlarının güvenlik stratejilerindeki öneminin yanı sıra MITRE ATT&CK, OWASP ve NIST gibi çerçeveler vurgulanmaktadır. Yapay zekâ tehdit tespiti, anomali analizi ve otomatik yanıt sistemlerindeki potansiyeli ile hem savunma hem de saldırı amaçlı kullanılmaktadır. Yapay zekâ destekli eğitim programları güvenlik duvarlarının ve Web Uygulaması Güvenlik Duvarlarının (WAF) etkinliğini artırmaktadır. Bununla birlikte, çalışmada sosyal mühendislik saldırıları, şifre kırma ve deepfakes gibi kötüye kullanım potansiyeli de tartışılmaktadır. Python Pytrends kütüphanesi ve Google Trends verileri kullanılarak siber güvenlik trend analizleri gerçekleştirilmekte ve önemli siber güvenlik trendlerini belirlemek ve görselleştirmek için TF-IDF yöntemi kullanılmaktadır. Çalışmada ayrıca otonom siber güvenlik sistemleri, kuantum kriptografi ve gizliliği artıran teknolojilerin potansiyel etkileri de tartışılmaktadır. Güvenlik uyum yönetiminin rolü ile yapay zekâ ve makine öğreniminin gelecekteki potansiyel etkileri de incelenmektedir.

1. Giriş

Siber güvenlik, bilgi sistemlerini, ağları ve verileri güvence altına almak için kullanılan çeşitli yöntem ve teknolojilerin incelenmesidir. Siber güvenlik alanındaki en acil sorunlardan biri, bir sistemin güvenliğini ihlal etmeye yönelik kasıtlı girişimler olan siber tehditlerdir. Stallings'in (2018) belirttiği

1 Dr. Öğr. Üyesi, Bilecik Şeyh Edebali Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, ORCID: 0000-0001-8455-5625, huseyin.parmaksiz@bilecik.edu.tr

https://doi.org/10.58830/ozgur.pub498.c2091

üzere; saldırganlar hassas bilgileri çalmak veya yayınlamak için kötü amaçlı yazılım, fidye yazılımı, sosyal mühendislik ve veri ihlallerini kullanmaktadırlar. Veri ihlalleri, yetkisiz erişim nedeniyle hassas bilgilerin çalınması veya yayınlanmasını içerir ve istismar olasılığı yüksektir. Bilgisayar korsanlığı, kötü amaçlı amaçlarla bilgisayar sistemlerine yetkisiz erişim sağlama eylemi olarak ifade edilmektedir. Andress ve Winterfeld (2013) siber savaşın karmaşık yapısını ve bunun güvenlik uygulayıcıları üzerindeki etkilerini inceleyerek bu alandaki tehditlerin sürekli evrildiğini vurgulamaktadırlar. Siber güvenliğin temel amacı, bu tehditleri önlemek ve etkilerini en aza indirmektir.

Siber güvenlik teknolojileri ve teknik operasyonlar, sistem güvenliğini ve tehdit önlemeyi sağlamak için çok önemlidir. Şifreleme ve kriptografi, verilere yalnızca yetkili kullanıcılar tarafından erişilebilmesini sağlayan depolama teknolojileridir. Güvenlik duvarları, ağ bağlantılarını izlemek ve istenmeyen erişimi önlemek için temel güvenlik tekniklerini uygulamaktadır. Saldırı tespit sistemleri (IDS) ve saldırı önleme sistemleri (IPS), düşmanca süreçleri belirleyerek engellemektedir (Singh, 2023). Sıfırıncı gün güvenlik açıkları, saldırganlar için önemli bir fırsat sunmaktadır. Dağıtılmış hizmet reddi saldırıları (DDoS), yoğun trafik nedeniyle bir sistemi çalışmaz hale getirebilir. Kimlik doğrulama ve yetkilendirme, güvenlik sistemlerinde kritik kavramlardır (Zargar, Joshi, & Tipper, 2013); erişim kontrolü (AC) (De Capitani di Vimercati, Paraboschi, & Samarati, 2003), kaynaklara kimin erişebileceğini yönetmektedir. Bu yaklaşımlar ve teknolojiler, sistem güvenliği ve tehdit önlemenin temelini oluşturmaktadır.

Siber güvenlik planları ve politikaları, bir kuruluşun dijital varlıklarını korumak için kritik öneme sahiptir. Risk yönetimi, olası tehditleri tespit ederek bunları azaltmak için uygun önlemleri uygulamaktadır. Bir ihlal durumunda, hızlı bir şekilde yanıt vermek üzere tasarlanmış sistemlerle olay müdahalesi esastır. Yönetim kavramları siber güvenlik prosedürlerini yönetirken uyumluluk politikaları yasal ve düzenleyici standartları karşılamaktadır. Tehdit istihbaratı, olası riskleri belirleyerek bunlar hakkında bilgi verir ve proaktif güvenlik eylemlerini mümkün kılar. Siber güvenlik önlemleri siber saldırıları önlerken adli teknikler siber suçları araştırır ve failleri belirler. Bu süreçlerin başarısı, sistemlerin dayanıklılığına yakından bağlıdır. Gizlilik ilkeleri, kişisel verileri koruyarak kullanıcı güvenliğini ve gizliliğini vurgular. Bu stratejik teknikler, siber güvenlik yönetiminde kapsamlı bir savunma sağlamaktadır.

Akademik araştırma ve teknikler açısından, siber güvenlik uygulamalarının etkinliğini artırmak için oluşturulan birçok kavram ve teknik yaklaşım, mevcut güvenlik altyapılarının geliştirilmesinde hayati öneme sahiptir.

Çerçeve, bu uygulamaların metodik bir şekilde uygulanmasını garanti ederken; modelleme yaklaşımı tehdit ve sistem simülasyonu yoluyla olası güvenlik açıklarının erken keşfedilmesini sağlar. Simülasyon yaklaşımları, gerçek dünya durumlarını simüle ederek güvenlik sistemlerinin verimliliğini değerlendirmek için kullanılır.

Yapay zekâ (YZ) ve makine öğrenimi büyük veri analiziyle entegre edildiğinde riskleri otomatik olarak belirleyip sınıflandırarak insan müdahalesine olan ihtiyacı en aza indirerek siber güvenliği devrimleştirebilirler. Algoritmalar, büyük veri kümelerini değerlendirmek, olası riskleri belirlemek ve güvenlik süreçlerini geliştirmek için gereklidir. Dahası, YZ destekli tespit sistemleri, anormal faaliyetleri hızla tanıyarak güvenlik ihlallerini önlemek için mükemmel bir teknik sağlar. YZ sistemleri, saldırı türlerini tahmin ederek proaktif risk azaltımı sağlar. Bu entegre yaklaşım, siber güvenliğin sürekli değişen doğasını ele almak için gereken esnek ve dinamik çözümleri sunmaktadır.

Güncel siber güvenlik trendleri, teknoloji hızla ilerledikçe güvenlik yöntemlerini değiştirmektedir. Bulut güvenliği, bulut tabanlı hizmetleri korumak için teknikler uygulayarak veri gizliliği ve erişim kontrolü zorluklarına önemli katkılarda bulunmaktadır. Aynı zamanda, nesnelerin interneti (IoT) güvenliği, bağlantılı cihazların sayısının artması nedeniyle bu cihazların güvenliğini güvence altına almak için yeni yolların geliştirilmesini gerektirmektedir. Blockchain güvenliği, dağıtılmış defter teknolojisinin entegrasyonunu kolaylaştırdığı için veri bütünlüğünü sağlamak için mükemmel bir seçenek olmaktadır (Banerjee, Lee, & Choo, 2018). Buna karşılık; kuantum kriptografisi, klasik şifreleme yaklaşımlarından daha sağlam bir güvenlik mimarisi oluşturmak için kuantum mekanik kavramları kullanmaktadır. Siber güvenlikteki YZ, tehdit algılama ve yanıt operasyonlarını otomatikleştirerek güvenlik analistlerinin verimliliğini artırmaktadır. Sıfır Güven Mimarisi, varsayılan olarak her kullanıcıya ve cihaza güvenmeme yaklaşımını benimseyerek güvenlik duvarlarını geliştirmektedir. Siber-fiziksel sistemlerin fiziksel ve dijital dünyalara entegrasyonu yeni güvenlik endişeleri yaratır; bu ortamda, uç bilgi işlem güvenliği, veri işleme ve depolama faaliyetlerini güvence altına almak için önemli bir konu olarak ortaya çıkmaktadır. Ayrıca, içeriden gelen saldırılar ve gelişmiş sürekli tehditler (APT), siber güvenlik çözümlerini karmaşık hale getirir (Chen, Desmet, & Huygens, 2014). Bu dinamik ve karmaşık değişimler, siber güvenliğin sürekli değişen doğasını yansıtarak daha dayanıklı ve uyarlanabilir güvenlik çözümlerine olan ihtiyacı vurgulamaktadır.

2. Siber Güvenlikte Tehditler ve Koruma Yöntemleri

Saldırı vektörleri, sistemlere, ağlara veya cihazlara yetkisiz erişim elde etmek için kullanılan siber tehditlerdir. Kötü amaçlı yazılım, kimlik avı, zayıf parolalar ve sosyal mühendislik gibi taktikler kullanarak güvenlik açıklarını, insan hatalarını ve zayıflıkları hedef almaktadır (Stallings & Brown, 2015). Bu vektörleri anlamak, tehditleri erken tespit etmek ve etkili güvenlik önlemleri geliştirmek için çok önemlidir (Sunit & Nina, 2011). Saldırılara karşı korunmak için güçlü parolalar, çok faktörlü kimlik doğrulama, düzenli yazılım güncellemeleri, siber güvenlik eğitimi ve güvenli ağ bağlantılarının kullanılması gerekmektedir. Özellikle Wi-Fi ağlarının güvenliğini artırmak için güçlü şifreleme yöntemleri kullanılmalı, misafir ağları ayrı bir yapılandırma ile yönetilmeli ve ağda bağlı cihazların birbirinden izole edilmesi sağlanmalıdır.

Ayrıca, etkili bir güvenlik stratejisi için log kayıtları düzenli olarak tutulmalı (Schmidt, Phillips, & Chuvakin, 2012); bu kayıtlar, 5651 sayılı Kanun (Türkiye Cumhuriyeti, 2007) kapsamında gerektiği gibi günlüklerin saklanarak, geriye dönük tespit ve faillerin belirlenmesi için önemli bir kaynak oluşturmalıdır. Kod analizi süreçlerinde ise açık kaynak ve lisanslı ürünler kullanılarak programlama dillerine özgü güvenlik açıklarının tespit edilmesi hedeflenmelidir (McGraw, 2012). Bu savunmaları tanımak ve uygulamak, sağlam bir siber güvenlik stratejisinin önemli bir parçasıdır.

2.1. Tehditler

Siber güvenlikte tehditler, sistemlere yönelik saldırıları ve bilgi hırsızlığı girişimlerini içermektedir. Bu tehditlerle başa çıkmanın iki temel yöntemi; saldırgan güvenlik ve savunma güvenliğidir (Melis v.d., 2023). Saldırgan güvenlik stratejileri, sistemlerdeki zayıflıkları tespit edip gidermeyi amaçlayan proaktif yöntemler kullanmaktadır. Bu kapsamda penetrasyon testi, sosyal mühendislik saldırıları ve uygulama güvenliği testleri gibi yöntemler öne çıkmaktadır. Bu yaklaşımlar, sistemlerdeki olası zafiyetleri keşfetmek için yapılan saldırı simülasyonlarına dayanmaktadır.

Saldırı vektörleri, siber saldırganların bir ağa, sisteme veya cihaza zarar vermek ya da yetkisiz erişim sağlamak için kullandıkları yolları ifade etmektedir. Zararlı yazılım (malware), oltalama (phishing), zayıf şifreler, açık ağ bağlantıları ve sosyal mühendislik gibi yöntemler sıkça kullanılan saldırı vektörleri arasında yer almaktadır (Gupta, Singhal, & Kapoor, 2016). Bu vektörlerin anlaşılması saldırıların erken tespit edilmesi ve güvenlik önlemlerinin iyileştirilmesi açısından kritik öneme sahiptir.

Siber güvenlik alanında sosyal mühendislik yöntemleri, bireyleri manipüle ederek gizli bilgi edinmeyi amaçlayan teknikler olarak öne çıkmaktadır. Bu yöntemler, kullanıcıların güvenini istismar ederek sistemlerin zayıf noktalarına ulaşılmasını kolaylaştırmaktadır. Bu bağlamda penetrasyon testleri uygulamaları, organizasyonların güvenlik durumunu değerlendirmek için kritik rol oynamaktadır (Wang, Sun, & Zhu, 2020). Bu testler, potansiyel zafiyetleri belirlemek amacıyla sistemlerin özenle analiz edilmesini sağlamaktadır. Botnet'ler, kontrol altına alınmış çok sayıda cihazdan oluşan ağlar olarak Dağıtık Hizmet Reddi (DDoS), siber saldırılarda geniş bir yelpazede kullanılmakta ve ciddi güvenlik tehditleri oluşturabilmektedir. Sosyal mühendislik testlerine yönelik çeşitli araçlar da bulunmaktadır. Kali Linux işletim sistemi üzerinde çalışan popüler bir araç olan Social Engineering Toolkit (SET) kullanıcıları kandırmaya yönelik senaryolar geliştirmeyi kolaylaştırmaktadır (Pavković & Perkov, 2011). Metasploit Framework, hem penetrasyon testlerinde hem de sosyal mühendislik saldırılarında kullanılabilecek kapsamlı bir platform olarak yer almaktadır.

2.2. Siber Güvenlik Hizmeti Olarak (Cyber Security as a Service-CSaaS)

Siber Güvenlik Hizmeti (CSaaS), siber güvenlik tehditlerinin çeşitlenmesi ve değişmesi nedeniyle giderek daha popüler hale gelmektedir. CSaaS, Güvenlik ve İzleme Yönetimi, Uç Nokta Güvenliği, Ağ Güvenliği, Veri Güvenliği, Kimlik ve Erişim Yönetimi, Yönetilen Algılama ve Yanıt (MDR), Güvenlik Açığı Yönetimi ve Güvenlik Uyumluluk Yönetimi dahil olmak üzere çeşitli güvenlik katmanları sunmaktadır (Morris et v.d., 2023). Bu hizmetler, tehditlerin erken tespiti ve yönetimi, cihazların korunması, ağ güvenliği çözümleri, veri şifreleme, veri kaybı önleme ve bulut politikaları sağlamaktadır. Ayrıca şirketlerin siber güvenliklerini güvence altına alarak riskleri azaltmalarına yardımcı olmaktadır. Hizmetler arasında varlık yokluğu, artırılmış risk parlaklığı ve yama yönetimi gibi özellikler de bulunmaktadır. Genel olarak, CSaaS şirketlerin güvenlik harcamalarını daha etkili bir şekilde karşılamalarına yardımcı olmaktadır.

2.3. Koruma Yöntemleri

Siber güvenliğin güçlendirilmesi amacıyla bir dizi strateji uygulanmakta ve çeşitli araçlar kullanılmaktadır. Bu bağlamda tehdit istihbaratı, güvenlik açığı yönetimi, ağ segmentasyonu ve felaket kurtarma planları gibi savunma stratejileri hem saldırganların hem de savunma yaklaşımlarının tamamlayıcı unsurları olarak önemli bir rol oynamaktadır. Etkili korunma yöntemleri arasında güçlü şifrelerin ve çok faktörlü kimlik doğrulamanın kullanılması

(Ometov v.d., 2018), yazılımların güncel tutulması, çalışanların siber güvenlik tehditlerine karşı eğitilmesi ve güvenli ağ bağlantılarının sağlanması yer almaktadır. Bu stratejiler, organizasyonların tehditlere karşı güçlü bir savunma oluşturmasına olanak tanırken saldırganların yöntemlerine karşı kapsamlı bir siber güvenlik yaklaşımı sunmaktadır.

Çalışanların düzenli eğitim programları ile bilinçlendirilmesi, sosyal mühendislik saldırılarına karşı en etkili savunma yöntemlerinden biridir ve bunlar insan hatası kaynaklı risklerin azaltılmasına da katkı sağlar. Ayrıca; güvenlik duvarları ve izleme sistemleri, ağ güvenliği kapsamında potansiyel tehditlerin erken tespitine olanak tanırken; penetrasyon testleri, sistemlerin zayıf noktalarının belirlenmesi ve bu zayıflıkların giderilmesi açısından kritik bir öneme sahiptir (Artsın & Parmaksız, 2023). Güvenli erişim yönetimi kimlik doğrulama ve yetkilendirme süreçlerini güçlendirerek yetkisiz erişimlerin önüne geçmektedir. Tüm bu yöntemler, organizasyonların siber güvenliklerini proaktif bir yaklaşımla artırırken sürekli gelişen tehditlere karşı da daha dirençli hale gelmelerini sağlamaktadır.

Sistemleri yöneten personelin, cihazların ve sistemlerin güncel tutulması siber güvenlik açısından büyük önem taşımaktadır. Bu süreç, güvenlik yamalarının düzenli olarak uygulanması ile sağlanmalıdır. Yazılım güncellemeleri ve güvenlik yamaları, bilinen güvenlik açıklarını kapatarak kötü niyetli saldırganların sistemlere sızma olasılığını azaltmaktadır. Güncel yazılımlar, yeni güvenlik tehditlerine karşı koruma sağlamak için en son güvenlik önlemlerini içermektedir. Sistem yöneticileri, tüm cihazların ve uygulamaların güncellenmesini sağlamak için düzenli bakım planları oluşturmalı ve bunları titizlikle uygulamalıdır. Bu sayede organizasyonlar, siber saldırılara karşı daha dayanıklı hale gelir ve veri güvenliğini artırarak siber tehditlerin etkisini minimize edebilirler. Ayrıca, güvenlik yamalarının zamanında uygulanması, düzenleyici uyumluluk gerekliliklerini karşılamada da kritik bir rol oynamaktadır.

2.4. Siber Güvenlikte Uzmanlık Sertifikalarının Rolü

Siber güvenlik risklerine karşı etkili bir şekilde mücadele edebilmek için, bireylerin deneyim, profesyonel kimlik bilgileri ve teknik bilgi ve yeteneklere sahip olmaları gerekmektedir. Bu bağlamda, çeşitli sertifikalar, uzmanların yetkinliklerini artırarak siber güvenlik alanında daha etkili olmalarını sağlamaktadır.

Sertifikalı Etik Hacker (CEH) sertifikası, etik bilgisayar korsanlarının sistem açıklarını tespit etme ve bu açıkları etik normlara uygun olarak simüle edilmiş saldırılarla kapatma kapasitesini geliştirmektedir. CEH

sertifikası, siber suçluların stratejilerini anlamayı ve bu stratejilere karşı savunma mekanizmaları geliştirmeyi öğretmektedir (Graves, 2010). Saldırgan Güvenlik Sertifikalı Profesyonel (OSCP) programı, siber güvenlik uzmanlarına pratik saldırı taktikleri sunarak savunma mekanizmaları oluşturma ve saldırı yollarını tahmin etme yeteneklerini geliştirmektedir. OSCP, uygulamalı bir sınav süreci ile katılımcıların penetrasyon testi becerilerini gerçek dünya senaryolarında kullanmalarını sağlamaktadır. CompTIA PenTest+ sertifikası ise penetrasyon testi, güvenlik açığı değerlendirmesi ve ağ güvenliği yönetimi konularında bilgi sağlayarak sistem korumasını güçlendirmektedir. Bu sertifika, özellikle orta düzeyde beceriye sahip siber güvenlik profesyonelleri için uygundur ve güvenlik açıklarını yönetme becerilerini geliştirmektedir. Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı (CISSP) sertifikası, bilgi güvenliği mimarisi, operasyonları ve risk yönetimi alanlarında kapsamlı bilgi sunarak güvenli ağ yapılandırmaları ve çok faktörlü kimlik doğrulama gibi stratejilerin kullanımını teşvik eder. CISSP, profesyonel itibarı arttıran uluslararası düzeyde tanınan bir sertifikadır (Davri v.d., 2021). GIAC Penetration Tester (GPEN) sertifikası, penetrasyon testi metodolojileri konusunda derinlemesine bilgi sağlayarak Wi-Fi ağ güvenliği için kritik koruma stratejilerine odaklanmaktadır. GPEN sertifikası, yasal konularla başa çıkma yeteneği de dahil olmak üzere kapsamlı bir eğitim sunmaktadır.

Türk Standartları Enstitüsü (TSE), sızma testi yapan firmalar için TSE 13638 standardına dayalı bir sertifikasyon sunmaktadır. Bu sertifika, firmaların belirli kalite ve güvenlik standartlarına uygun olarak sızma testleri gerçekleştirdiğini kanıtlamaktadır (Doğan & Karacan, 2022). TSE 13638 standardı, Türkiye'deki sızma testlerinin belirli bir güvenlik seviyesinde yapılmasını sağlayarak bu testlerin nasıl gerçekleştirileceği, hangi araçların kullanılacağı ve sonuçların nasıl raporlanacağı konusunda rehberlik etmektedir. TSE onaylı sızma testi belgesi, işletmelerin bilgi sistemlerini ulusal standartlara uygun bir şekilde değerlendirdiğini göstermektedir. Bu belgeyi almak için, firmaların TSE'nin belirlediği kriterlere göre testler yapması ve sonuçları TSE'ye raporlaması gerekmektedir. Bu sertifikalar, siber güvenlik uzmanlarının siber tehlikelerini erken fark etmelerini ve etkili savunma stratejileri geliştirmelerini sağlayarak kariyerlerinde önemli avantajlar elde etmelerine yardımcı olmaktadır.

3. Siber Güvenlikte Açık Kaynak Yazılımlar

Açık kaynak yazılımlar, siber güvenlik alanında maliyet etkin çözümler sunarak organizasyonların güvenliğini artırmalarına yardımcı olmaktadır. Bu araçlar hem tehditlerin tespit edilmesi hem de olaylara hızlı yanıt verilmesi

açısından kritik öneme sahiptir. Siber güvenlik uzmanları, bu yazılımları kullanarak sistemlerini daha iyi koruyabilir ve potansiyel zayıf noktaları belirleyebilirler.

3.1. Açık Kaynaklı Yazılımlar

Siber güvenlik alanında kullanılan çeşitli açık kaynak yazılımlar, farklı işlevleri ve kullanım yapılarıyla kuruluşların güvenliğini artırmada önemli katkılar sağlamaktadır. Bu yazılımlar kimlik ve erişim yönetiminden ağ güvenliğine, tehdit izleme ve yanıta kadar geniş bir yelpazede hizmet sunmaktadır. Kimlik ve erişim yönetimi (IAM) için güçlü bir araç olan Keycloak, kullanıcıların kimlik doğrulama ve yetkilendirme süreçlerini etkin bir şekilde yönetmelerine olanak tanır; çok faktörlü kimlik doğrulama (MFA) ve sosyal oturum açma gibi özellikleriyle kullanıcıların tek bir kimlik bilgisi setiyle birden fazla uygulamaya erişimini sağlamaktadır. Açık kaynaklı ayrıcalıklı erişim yönetimi (PAM) çözümleri, şirket güvenliğini iyileştirmek ve yetkisiz erişimi engellemek için kritik öneme sahiptir.

FreeIPA, LDAP, Kerberos ve DNS gibi teknolojiler aracılığıyla kullanıcı erişimini ve ayrıcalıklarını yönetirken kimlik doğrulama, yetkilendirme ve muhasebe bilgilerini merkezileştiren bir güvenlik bilgi yönetim sistemidir. HashiCorp Vault, hassas verileri depolamak ve korumak için popüler bir çözümdür; CyberArk Conjur ise DevOps ortamları için tasarlanmıştır.

Ağ Erişim Kontrolü (NAC) sağlayan PacketFence, yetkisiz erişimi önleyerek güvenli ağlara erişimi düzenlemekte ve cihazları ağa bağlanmadan önce kimlik doğrulaması yaparak ağ güvenliğini artırmaktadır. Wazuh, güvenlik bilgi ve olay yönetimi (SIEM), genişletilmiş algılama ve yanıt (XDR) çözümleri sunarak tehdit izleme ve yanıt süreçlerini etkinleştirirken (Sridharan & Kanchana, 2022). OpenCTI, siber tehdit istihbaratı yönetimi için bir platform olarak tehdit bilgilerini toplamakta, analiz etmekte ve dağıtmaktadır.

Velociraptor, uç nokta görünürlüğü ve toplama aracılığıyla derinlemesine analizler gerçekleştirirken GoAccess, gerçek zamanlı web günlüğü analizcisi olarak kullanıcı davranışlarını izleyerek olası tehditleri tespit etmektedir. Syncthing, kullanıcıların dosyalarını güvenli bir şekilde senkronize etmelerini sağlarken TacacsGUI, TACACS+ protokolü üzerine inşa edilen bir erişim kontrol sunucusu olarak kimlik doğrulama, yetkilendirme ve hesap yönetimini merkezi olarak gerçekleştirmektedir. T-Pot, birden fazla honeypot çözümünü entegre eden kapsamlı bir platform olarak kötü amaçlı faaliyetleri tespit etme ve saldırganların tekniklerini anlama konusunda kritik bir öneme sahiptir. Son olarak SELKS, Debian tabanlı bir IDS, IPS

ve ağ güvenliği izleme platformu olarak ağ trafiğini izleyerek potansiyel tehditleri tespit etmeye ve ağ faaliyetlerini analiz etmeye olanak tanımaktadır (Baykara & Daş, 2019). Bu yazılımlar, açık kaynaklı yapıları sayesinde geniş bir topluluk tarafından desteklenmekte ve sürekli olarak geliştirilerek siber güvenlik alanındaki yenilikleri takip etmeyi kolaylaştırmaktadır.

3.2. Çerçeveler

Açık Siber Tehdit İstihbaratı (OpenCTI), siber tehdit istihbaratını yönetmek için kullanılan açık kaynaklı bir platformdur. Kullanıcıların tehdit verilerini merkezi bir sistemde toplamasına, analiz etmesine ve paylaşmasına olanak tanıyarak tehditlere karşı daha etkili bir savunma geliştirmelerine yardımcı olur.

MITRE ATT&CK, siber saldırı tekniklerinin, taktiklerinin ve prosedürlerinin sistematik bir kütüphanesi olarak güvenlik uzmanlarının saldırı senaryolarını daha iyi anlamalarını ve savunma stratejilerini geliştirmelerini sağlamakta önemli bir kaynak işlevi görmektedir (Mitre Corporation, 2020).

Açık Web Uygulaması Güvenlik Projesi (OWASP) ise web uygulama güvenliği konularında en iyi uygulamaları ve standartları geliştiren bir topluluktur; "OWASP Top Ten" gibi projelerle, uygulama güvenliğinde yaygın olan zayıflıkları belirleyerek bu zayıflıklarla başa çıkma yöntemleri sunmaktadır (Helmiawan et al., 2020).

Açık Güvenlik Açığı ve Değerlendirme Dili (OVAL), güvenlik açıklarının ve sistem konfigürasyonlarının tanımlanması ve değerlendirilmesi için standart bir format sağlayarak, güvenlik uzmanlarının zafiyetleri sistematik bir şekilde analiz etmelerine yardımcı olmaktadır.

Güvenlik açıklarının ciddiyetini değerlendirmek için kullanılan bir standart olan Ortak Güvenlik Açığı Puanlama Sistemi (CVS), güvenlik uzmanlarının önceliklendirme yapmalarına yardımcı olmaktadır. Yaygın Güvenlik Açıkları ve Maruz Kalmalar (CVE), belirli güvenlik açıklarını tanımlamak için kullanılan bir veri tabanıdır ve zafiyetlerin genel tanımlarını sunmaktadır. Ortak Zayıflık Sayımı (CWE) ise yazılım zayıflıklarını sınıflandırmak için kullanılan bir referans kaynağıdır. Ayrıca yazılım güvenliği konularında farkındalığı artırmaya yönelik önemli bilgiler sağlamaktadır (Martin, 2019).

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), siber güvenlik alanında en iyi uygulamaları ve standartları belirleyen önemli bir kuruluş olarak öne çıkar. NIST'in Siber Güvenlik Çerçevesi, organizasyonların siber risklerini yönetmelerine yardımcı olmak için bir dizi rehberlik ve araç

sunar. Bu çerçeve, siber güvenlik stratejilerini geliştirmek ve uygulamak için kapsamlı bir yol haritası sağlar. Bu araçlar ve çerçeveler, mevcut siber güvenlik çözümlerini tamamlayarak organizasyonların güvenlik stratejilerini güçlendirmelerine katkı sağlamakta; böylece siber güvenlik alanında daha kapsamlı bir anlayış sunmaktadır (Schlenoff, Scott, & Balakirsky, 2011).

3.3. Zafiyet Analizi

Penetrasyon testi ve güvenlik açığı taraması için kullanıcı dostu bir platform olan Archery, insanların sistemlerini incelemelerini ve kusurları belirlemelerini sağlar. OpenVAS, ağları tarayan ve kullanıcılara güvenlik durumunu analiz etmek için güncel bir veritabanı sağlayan açık kaynaklı bir güvenlik açığı değerlendirme sistemidir. Vuls, açık kaynaklı ve ajan gerektirmeyen bir güvenlik açığı tarayıcısı olarak, siber güvenlik alanında kritik bir rol oynamaktadır.

Ulusal Güvenlik Açığı Veritabanı (NVD), OVAL gibi kaynaklardan elde edilen bilgilerle çalışarak sistemlerdeki potansiyel güvenlik açıklarını tespit eder ve bu açıkların etkilerini analiz eder. Vuls, organizasyonların güvenlik açıklarını proaktif bir şekilde yönetmelerine olanak tanırken, tarama süreçlerini basit ve etkili hale getirir. Graylog, makine öğrenimini kullanarak anormallik algılama ve olay yanıt prosedürlerini geliştiren merkezi bir günlük yönetimi ve güvenlik analitiği çözümüdür. Suricata, ağları gerçek zamanlı olarak analiz eden ve çoklu iş parçacığı yeteneği sayesinde yüksek hızlarda çalışabilen yüksek performanslı, açık kaynaklı bir IDS/IPS'dir. Cuckoo Sandbox, kullanıcıların izole bir ortamda şüpheli dosyaları izlemelerine ve sonuçlarını öğrenmelerine olanak tanıyan bir kötü amaçlı yazılım analiz aracıdır. Bu teknolojiler, sibergüvenlikteki kapsamlı değerlendirme ve analiz prosedürleri aracılığıyla sistem güvenliğinin iyileştirilmesine yardımcı olmaktadır (Wiley, 2008).

4. Siber Güvenlikte Yapay Zekâ, Trend Analizleri ve Uyum Yönetimi

YZ, bilgisayarlarda insan zekâsını taklit eden ve robotların daha önce insanlar tarafından yapılan görevleri yerine getirmesini sağlayan bir teknolojidir. 1950'de Alan Turing'in fikirleriyle başlayan YZ, siber güvenlikte önemli ilerlemelere neden olmaktadır (Muggleton, 2014).

YZ, büyük veri kümelerini analiz edebilir, tehditleri daha etkili bir şekilde belirleyebilir, yanlış pozitifleri ortadan kaldırabilir ve gerçek dünya tehlikelerine göre eylemleri önceliklendirebilir. Ayrıca şüpheli e-postaları tespit edebilir (Qabajeh, Thabtah, & Chiclana, 2018), sosyal mühendislik

saldırılarını simüle edebilir ve olaylarla ilgili verileri hızla değerlendirerek güvenlik ekiplerinin derhal yanıt vermesini sağlayabilir.

YZ, siber güvenlikte veri koruması ve maliyet tasarrufu için çok önemlidir ve bu da onu işletmeler için onu önceliklendirmektedir (Geluvaraj, Satwik, & Ashok Kumar, 2019). YZ destekli siber güvenlik ürünleri için küresel pazarın 2021'de 15 milyar dolardan 2030'a kadar 135 milyar dolara çıkması beklenmektedir.

4.1. Yapay Zekânın Siber Güvenlikte Rolü ve Uygulama Alanları

Günümüzde YZ, siber güvenlikte giderek daha önemli bir rol oynamaktadır. Hem saldırganlar hem de savunucular için bir silah olarak YZ, siber tehditlerin doğasını ve ele alınmasını kökten değiştirmektedir.

4.1.1. Siber Güvenlikte Yapay Zekânın İyiye Kullanımı

Çalışan eğitimi siber güvenlikte çok önemlidir. YZ destekli eğitim programları, personeli sosyal mühendislik saldırılarına daha iyi hazırlamak için kişiselleştirilmiş materyaller sunmaktadır. Araştırmalar, personel eğitimine yatırım yapmanın veri ihlallerinin maliyetini önemli ölçüde düşürebileceğini göstermiştir.

YZ, büyük veri analitiği ve makine öğrenimi tekniklerini kullanarak olası tehlikeleri hızla tespit edebilmektedir. Bu sistemler, olağan etkinlik kalıplarını değerlendirerek anormallikleri tespit edebilir ve saldırıları tahmin edebilir. YZ tabanlı sistemler, virüsleri ve şüpheli etkinlikleri tespit etmek için ağ trafiğini izleyebilmektedir.

Olay müdahalesi, YZ'nin önemli bir safhası olarak bilinmektedir. Bir güvenlik ihlali durumunda, YZ sistemleri tehlikeye atılan bilgisayarları hemen izole edebilmekte veya şüpheli IP adreslerini engelleyebilmektedir. Bu hızlı tepki mekanizması, insan hatasını azaltarak kurumsal güvenliği iyileştirmektedir (Steinke v.d., 2015).

Coroza, ModSecurity ve Naxsi (Garn et al., 2021) gibi YZ destekli güvenlik duvarları ve açık kaynaklı WAF'lar, gelen iletişimleri analiz ederek, potansiyel tehditleri belirleyerek ve gerçek zamanlı tehdit koruması için dinamik kurallar sağlayarak siber güvenliği iyileştirmektedir. Bu durum, kuruluşların dijital dönüşüm geçirirken stratejilerini yeniden düşünmelerini gerekli hale getirmektedir.

YZ gelişmeleri, kuruluşların veri güvenliği operasyonlarını optimize etmelerini sağlarken aynı zamanda ortaya çıkan tehditlerle başa çıkma kapasitelerini de artırmaktadır.

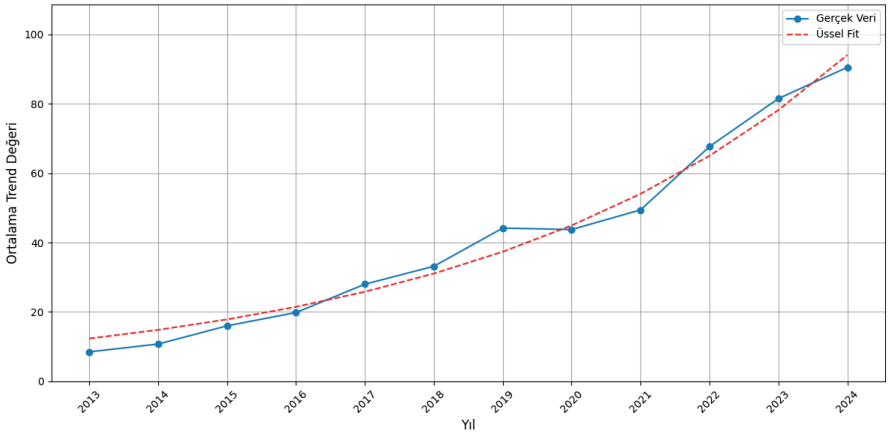
4.1.2. Siber Güvenlikte Yapay Zekânın Kötüye Kullanımı

Siber suçlular, sosyal mühendislik, parola kırma, deepfake ve veri zehirleme gibi çeşitli yöntemlerle YZ'yi kullanırlar. Ayrıca suçlular sosyal mühendislik yoluyla başkalarını etkilerler, kritik bilgileri ifşa ederler veya güvenlik ihlalleri gerçekleştirirler. YZ, bu saldırılarda otomasyonu iyileştirerek daha özel ve etkili mesajlaşma sağlar. Gelişmiş parola kırma algoritmaları verimliliği artırarak daha hızlı ve daha kesin tahminler yapılmasını sağlar.

Deepfake teknolojisi sahte ses ve video bilgilerinin yanı sıra sosyal mühendislik ve şantaj gibi dolandırıcılık taktikleri oluşturmak için kullanılmaktadır (Westerlund, 2019). Veri zehirleme, aldatıcı sonuçlar sağlamak için YZ sistemlerinin eğitim verilerinin kasıtlı olarak manipüle edilmesidir. Bu ise karar alma süreçleri üzerinde olumsuz bir etkiye sahiptir ve keşfi zorlaştırır. YZ'nin kötüye kullanılması, siber güvenlik tehditlerinin karmaşıklığını ve tehlikesini artırır.

4.2. Siber Güvenlik Trend Analizleri

Python Pytrends kütüphanesi aracılığıyla Google Trends web sitesinde sunulan sonuçları, Google Trends API'sini kullanarak analiz etmemizi kolaylaştırmaktadır (Hogue & DeWilde, 2023). Şekil 1'de bu kütüphane kullanılarak son on yılda siber güvenlik alanında değişim trendi verilmektedir.



Şekil 1. Pytrends ile Son 10 Yılın Siber Güvenlik Analizi

Web Of Science'ta siber güvenlik alanında son on yılda 821 yayın bulunmaktadır. Tablo 1'de en çok yayına sahip ilk on kategori verilmiştir.

Tablo 1. WOS ile Son 10 Yılın Siber Güvenlik Yayınlarının Dağılımı

WOS (Kategoriler)	Sayı	%
Bilgisayar Bilimleri Bilgi Sis.	241	%29.35
Mühendislik Elektrik Elektronik	196	%23.87
Telekomünikasyon	99	%12.06
Mühendislik Multidisipliner	62	%7.55
Uygulamalı Fizik	62	%7.55
Bilgisayar Bil. Disiplinler Arası Uygulamalar	58	%7.07
Bilgisayar Bilimleri Teori Yön.	58	%7.07
Kimya Analitik	49	%5.97
Enerji Yakıtları	49	%5.97
Bilgisayar Bilimleri Yapay Zekâ	46	%5.60

Terim Frekansı-Tersine Doküman Frekansı (TF-IDF), en temel ifade ile bir metin vektörleştirme yöntemidir. TF-IDF ile bir metindeki veya dizideki kelimelerin metinle ne kadar ilgili olduğunun hesaplanması gerçekleştirilmektedir (Bafna, Pramod, & Vaidya, 2016). TF-IDF Makine öğrenmesi, metin madenciliği, doğal dil işlemi gibi uygulamalarda sıkça kullanılmaktadır. Bu yöntem, bir belgede kelimenin kaç kez görüldüğü (TF) ve bir dizi belgede (farklı belgelerde) kelimenin ters belge sıklığı (IDF) ölçümlerini kullanmaktadır. TF-IDF yöntemiyle siber güvenlik alanında belirleyici önemli kelimeler Şekil 2'de kelime bulutu olarak sunulmaktadır.

Şekil 2. Siber Güvenlikteki Belirleyici Kelime Bulutu.

Siber güvenliğin artan önemi, günümüzde YZ'nin sağladığı yaratıcı çözümlerin yanı sıra çeşitli güncel metodolojilerinde oluşturulmasına olanak tanımaktadır (Lu, 2018). Bu bağlamda, otonom siber güvenlik sistemleri saldırıları otomatik olarak tespit etme ve bunlara yanıt verme kapasiteleriyle

öne çıkmaktadır. Bu sistemler, sürekli öğrenme yetenekleri sayesinde yeni tehditlere hızla yanıt verirken sistem güvenliğini güçlendirmede önemli bir rol oynamaktadır. Ayrıca, özellikle büyük dil modelleri olmak üzere yeni nesil YZ teknikleri, daha karmaşık ve ikna edici sosyal mühendislik saldırılarına olanak tanımaktadır. Bu tür saldırılar, insanların psikolojik durumlarını hedef alır ve daha büyük hedefli manipülasyon taktiklerinin kullanılmasına olanak tanımaktadır. Diğer yandan kuantum kriptografisi, kuantum bilgi teknolojisinin büyümesiyle birlikte, siber güvenlikte yenilikçi çözümlerin yaratılmasını sağlama potansiyeline sahiptir (Gisin, Ribordy, Tittel, & Zbinden, 2002). Bu yeni kriptografik teknolojiler, veri koruma prosedürlerini artırmak için YZ ile birleştirildiğinde güvenlik kontrollerinin etkinliğini büyük ölçüde iyileştirme potansiyeline sahiptirler. YZ ve kuantum teknolojileri, siber güvenlik stratejilerinin büyümesinde önemli bir rol oynar ve bu alandaki tehditlerle mücadele için yaratıcı ve etkili yöntemler sağlamaktadır (Nair, Deshmukh, & Tyagi, 2024).

4.3. Siber Güvenlik Uyum Yönetimi

Güvenlik uyumluluk yönetimi, bir kuruluşun bilgi güvenliği politikalarının düzenlemeler, endüstri standartları ve iç politikalarla uyumlu olmasını sağlamak için önemli bir etkendir. Risk yönetimi, yasal yükümlülükler, itibar koruması ve güven oluşturma için çok önemlidir.

4.3.1. Güvenlik Uyumluluk Yönetiminin Önemi

Güvenlik uyumluluk yönetimi, işletmelerin düzenleyici yükümlülükleri ve endüstri standartlarını karşıladıklarından emin olmaları için kritik derecede önemlidir. Sadece veri koruma düzenlemelerini güçlendirmekle kalmaz; aynı zamanda güvenlik risklerini azaltarak siber saldırılara karşı dirençli olmayı sağlamaktadır. Bu teknik ayrıca, şirketlerin güvenlik ihlallerinden kaynaklanan itibar zararını azaltarak kamu imajlarını korumalarına yardımcı olmaktadır. Dahası; güvenliğe ve gizliliğe bağlılık göstererek tüketici güvenini oluşturmaktadır. Güvenlik uyumluluk yönetimi ayrıca prosedürleri ve kontrolleri standart hale getirerek ve operasyonel verimliliği artırarak işletmelerin daha verimli ve sürdürülebilir bir şekilde çalışmasını sağlamaktadır. Temel güvenlik uyumluluk standartları ve kuralları, işletmelerin veri güvenliğini güvence altına almasına yardımcı olmaktadır.

Genel Veri Koruma Yönetmeliği (GDPR) veri işleme, depolama ve aktarımı için sıkı yönergeler belirlerken Türkiye'nin Kişisel Verilerin Korunması Kanunu (KVKK) yerel kısıtlamalarını içermektedir. Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS) güvenli kredi kartı işleme, depolama ve aktarımı için belirtilen gereksinimleri belirlemektedir.

ISO/IEC 27001, bilgi güvenliği yönetim sistemleri için kapsamlı bir çerçeve tanımlamaktadır. Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası (HIPAA), Amerika Birleşik Devletleri'nde sağlık bilgilerinin gizliliğini ve güvenliğini korumaktadır. SOC 2, hizmet işletmelerinin güvenlik, erişilebilirlik, işlem bütünlüğü, gizlilik ve mahremiyet kontrollerini değerlendirmektedir.

4.3.2. Güvenlik Uyumluluk Yönetimi Süreci

Güvenlik uyumluluk yönetimi süreci, veri güvenliğini iyileştirmenin ve işletmelerde yasal uyumluluğu sağlamanın sistematik bir adımı olarak bilinmektedir. Uygulanabilir kuralları ve endüstri standartlarını belirleyerek başlar, ardından kuruluşun güvenlik politikalarını, süreçlerini ve kontrollerini değerlendirir. Uygunsuzluk riskleri tanınır ve bunları azaltmak için yöntemler belirlenir. Güvenlik politikaları ve prosedürleri geliştirilir ve güncellenir, teknik ve idari güvenlik önlemleri alınır. Personelin uyumluluk standartlarını kavraması için düzenli eğitim ve farkındalık kampanyaları gerekmektedir. İzleme ve denetim aşaması, uyumluluk önlemlerinin sürekli izlenmesini ve periyodik denetimleri içermektedir. Sürekli geliştirme, düzenli uyumluluk durumu raporlaması ve denetim sonuçlarına dayalı iyileştirme stratejilerinin geliştirilmesini gerektirmektedir. Bu seviyeler, bir kuruluşun güvenlik durumunu iyileştirerek, yasal gerekliliklerini karşılamasına yardımcı olmaktadır.

4.3.3. Güvenlik Uyumluluk Yönetiminin Geleceği

Güvenlik uyumluluk yönetiminin geleceği, teknoloji ilerledikçe ve siber riskler daha yaygın hale geldikçe değişmektedir. YZ ve makine öğrenimi uyumluluk değerlendirme ve risk analizi prosedürlerinde kapsamlı bir şekilde uygulanacak ve sürekli uyumluluk doğrulama sistemlerine olanak tanıyacaktır. Otonom uyumluluk sistemleri, self servis uyumluluk yönetimi platformlarına olanak tanıyacak ve süreç verimliliğini artıracaktır. Küresel uyumluluk çerçeveleri, mevzuatı uluslar ve endüstriler arasında uyumlu hale getirirken; gizliliği artıran teknoloji (PET) veri gizliliğini koruyarak uyumluluğu garanti edecektir. Bu gelişmeler, güvenlik uyumluluk yönetimini işletmelerin yasal gereklilikleri karşılaması, riskleri yönetmesi ve itibarlarını koruması için kaçınılmaz bir prosedür haline getirmiştir. Proaktif, risk odaklı ve teknoloji destekli bir uyumluluk yönetimi yaklaşımı, firmaların dijital çağda güvenli ve karlı bir şekilde işlev görmesine yardımcı olabilecektir.

5. Sonuç

Bu çalışma, siber güvenlik alanının karmaşık ve sürekli gelişen doğasını kapsamlı bir şekilde ele almıştır. Araştırmamız, siber tehditlerin giderek daha sofistike hale geldiğini ve geleneksel güvenlik önlemlerinin artık yeterli olmadığını göstermektedir. Özellikle açık kaynak yazılımların siber güvenlik alanında sunduğu fırsatlar ve zorluklar, gelecekteki savunma stratejilerinin şekillenmesinde kritik bir rol oynayacaktır. Bu bağlamda, Keycloak, PacketFence, Wazuh gibi araçların etkin kullanımı, organizasyonların güvenlik duruşunu önemli ölçüde güçlendirebilir.

YZ teknolojilerinin siber güvenlik alanındaki uygulamaları hem savunma hem de saldırı perspektifinden incelenmiştir. Bulgularımız, YZ'nin tehdit tespiti, anomali analizi ve otomatik yanıt sistemlerinde devrim niteliğinde değişiklikler getirdiğini ortaya koymaktadır. Ancak, YZ'nin kötü niyetli aktörler tarafından da kullanılabileceği gerçeği, siber güvenlik profesyonellerinin sürekli olarak yeni stratejiler geliştirmesini zorunlu kılmaktadır.

Trend analizlerimiz, bulut güvenliği, IoT güvenliği ve kuantum kriptografisi gibi alanların gelecekte daha da önem kazanacağını göstermektedir. Bu gelişmeler, siber güvenlik eğitiminin ve farkındalığının tüm organizasyon seviyelerinde artırılması gerektiğini vurgulamaktadır. Ayrıca, güvenlik uyum yönetiminin geleceği, yasal düzenlemelerin ve endüstri standartlarının sürekli evrimiyle şekillenecektir.

Sonuç olarak, bu çalışma siber güvenliğin multidisipliner doğasını ortaya koyarak teknoloji, insan faktörü ve politika arasındaki karmaşık ilişkiyi vurgulamaktadır. Gelecekteki araştırmalar, bu alanlar arasındaki etkileşimi daha derinlemesine incelemeli ve bütünsel güvenlik çözümleri geliştirmeye odaklanmalıdır. Siber güvenliğin geleceği proaktif, adaptif ve işbirlikçi yaklaşımların benimsenmesine bağlı olacaktır. Bu bağlamda, sürekli eğitim, araştırma ve geliştirme faaliyetleri, siber tehditlere karşı etkili savunma stratejilerinin temelini oluşturacaktır.

Kaynakça

Andress, J., & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. *Elsevier*.

Artsın, M., & Parmaksız, H. (2023, October). Bilişim teknolojileri eğitiminde siber güvenlik: Zafiyet tarama ve sızma testlerinin önemi. *In 16. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu* (Eskişehir).

Bafna, P., Pramod, D., & Vaidya, A. (2016, March). Document clustering: TF-IDF approach. *In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 61-66). IEEE. https://doi.org/10.1109/ICEEOT.2016.7754750

Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: A position paper. *Digital Communications and Networks, 4*(3), 149-160. https://doi.org/10.1016/j.dcan.2017.10.006

Baykara, M., & Daş, R. (2019). Saldırı tespit ve engelleme araçlarının incelenmesi. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 10*(1), 57-75. https://doi.org/10.24012/dumf.449059

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. *In Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014*, Aveiro, Portugal, September 25-26, 2014. Proceedings 15 (pp. 63-72). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44885-4_5

Davri, E. C., Darra, E., Monogioudis, I., Grigoriadis, A., Iliou, C., Mengidis, N., ... & Farah, M. A. B. (2021, July). Cyber security certification programmes. *In 2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 428-435). IEEE. https://doi.org/10.1109/CSR51186.2021.9527974

De Capitani di Vimercati, S., Paraboschi, S., & Samarati, P. (2003). Access control: Principles and solutions. *Software: Practice and Experience, 33*(5), 397-421. https://doi.org/10.1002/spe.513

Doğan, Ö., & Karacan, H. (2022). Türkiye'deki e-ticarete özgü blokzincir tabanlı dijital kimlik güven çerçevesi önerisi. *Bilgi Yönetimi, 5*(2), 256-279. https://doi.org/10.33721/by.1113558

Garn, B., Lang, D. S., Leithner, M., Kuhn, D. R., Kacker, R., & Simos, D. E. (2021, April). Combinatorially XSSing web application firewalls. *In 2021 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)* (pp. 85-94). IEEE. https://doi.org/10.1109/ICSTW52544.2021.00026

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. *In International Conference on Computer Net-*

works and Communication Technologies: ICCNCT 2018 (pp. 739-747). Springer Singapore. https://doi.org/10.1007/978-981-10-8681-6_67

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics, 74*(1), 145-195. https://doi.org/10.1103/RevModPhys.74.145

Graves, K. (2010). CEH certified ethical hacker study guide. John Wiley & Sons.

Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. *In 2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 537-540). IEEE. https://doi.org/10.1109/CCAA.2016.7813778

Helmiawan, M. A., Firmansyah, E., Fadil, I., Sofivan, Y., Mahardika, F., & Guntara, A. (2020, October). Analysis of web security using open web application security project 10. *In 2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE. https://doi.org/10.1109/CITSM50537.2020.9268856

Hogue, J., & DeWilde, B. (2023). pytrends: Pseudo API for Google Trends. https://pypi.org/project/pytrends (E.T.: 20.10.2024).

Lu, Y. (2018). Cybersecurity research: A review of current research topics. *Journal of Industrial Integration and Management, 3*(04), 1850014. https://doi.org/10.1142/S2424862218500148

Martin, B. (2019). Common Vulnerabilities Enumeration (CVE), Common Weakness Enumeration (CWE), and Common Quality Enumeration (CQE): Attempting to systematically catalog the safety and security challenges for modern, networked, software-intensive systems. *ACM SIGAda Ada Letters, 38*(2), 9-42. https://doi.org/10.1145/3375408.3375410

Melis, A., Al Sadi, A., Berardi, D., Callegati, F., & Prandini, M. (2023). A systematic literature review of offensive and defensive security solutions with software defined network. *IEEE Access, 11*, 93431-93463. https://doi.org/10.1109/ACCESS.2023.3276238

McGraw, G. (2012). Software security: Building security in. *Datenschutz und Datensicherheit-DuD, 36*(9), 662-665.

Mitre Corporation. (2020). ATT&CK® framework for enterprise: Techniques used by adversaries and mitigations for them. Retrieved from https://attack.mitre.org/

Morris, J., Tatschner, S., Heinl, M. P., Heinl, P., Newe, T., & Plaga, S. (2023). Cybersecurity as a service. *In Cybersecurity Vigilance and Security Engineering of Internet of Everything* (pp. 141-161). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45162-1_9

Muggleton, S. (2014). Alan Turing and the development of artificial intelligence. *AI Communications, 27*(1), 3-10.

Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. *In Automated Secure Computing for Next-Generation Systems* (pp. 83-114). Springer. https://doi.org/10.1002/9781394213948.ch5

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography, 2*(1), 1. https://doi.org/10.3390/cryptography2010001

Pavković, N., & Perkov, L. (2011, May). Social engineering toolkit—A systematic approach to social engineering. *In 2011 Proceedings of the 34th International Convention MIPRO* (pp. 1485-1489). IEEE.

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review, 29*, 44-55. https://doi.org/10.1016/j.cosrev.2018.05.003

Schlenoff, C., Scott, H., & Balakirsky, S. (2011). Performance evaluation of intelligent systems at the National Institute of Standards and Technology (NIST). *International Test and Evaluation Association (ITEA) Journal, 32*(1), 59-67.

Schmidt, K., Phillips, C., & Chuvakin, A. (2012). Logging and log management: The authoritative guide to understanding the concepts surrounding logging and log management. *Newnes.*

Fuchsberger, A. (2005). Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report, 10*(3), 134-139. http://dx.doi.org/10.5121/ijcnc.2014.6407

Sridharan, A., & Kanchana, V. (2022, November). SIEM integration with SOAR. *In 2022 International Conference on Futuristic Technologies (INCOFT)* (pp. 1-6). IEEE. https://doi.org/10.1109/INCOFT55651.2022.10094537

Stallings, W., & Brown, L. (2015). Computer security: Principles and practice. *Pearson*.

Stallings, W. (2018). Effective cybersecurity: A guide to using best practices and standards. Addison-Wesley Professional.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., ... & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy, 13*(4), 20-29. https://doi.org/10.1109/MSP.2015.71

Sunit, B., & Nina, G. (2011). Cyber security: Understanding cybercrimes, computer forensics and legal perspectives. *Wiley India*.

Türkiye Cumhuriyeti. (2007). 5651 sayılı Kanun: İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele hakkında kanun. Resmî Gazete. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5 (E.T.: 20.10.2024).

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access, 8*, 85094-85115. https://doi.org/10.1109/ACCESS.2020.2992807

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11). https://doi.org/10.22215/timreview/1282

Wiley, J. (2008). Security engineering: A guide to building dependable distributed systems (2nd ed., pp. 239-274).

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046-2069. https://doi.org/10.1109/SURV.2013.031413.00127