Derinlemesine Güvenlik Stratejisi

Siber Güvenlik Profesyonel Görev Tanımı El Kitabı

İÇİNDEKİLER

1. GENEL BAKIŞ

Chief Information Security Officer (CISO)

Cyber Incident Responder

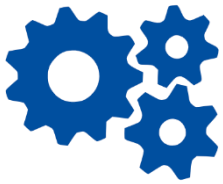
Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

Cybersecurity Educator



Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator

Penetration Tester

2. PROFİLLER

2.1 BİLGİ GÜVENLİĞİ BAŞKANI (CISO)

Profil başlığı	Baş Bilgi Güvenliği Görevlisi (CISO)
Alternatif Başlık(lar)	Siber Güvenlik Programı Direktörü Bilgi Güvenliği Sorumlusu (ISO) Bilgi Güvenliği Müdürü Bilgi Güvenliği Başkanı BT/BİT Güvenlik Görevlisi
Özet beyanı	Dijital sistemlerin, hizmetlerin ve varlıkların yeterince güvenli ve korunmasını sağlamak için bir kuruluşun siber güvenlik stratejisini ve uygulamasını yönetir.
Misyon	Siber güvenlik vizyonunu, stratejisini, politikalarını ve prosedürlerini tanımlar, sürdürür ve iletir. Kuruluş genelinde siber güvenlik politikasının uygulanmasını yönetir. Dış otoriteler ve meslek kuruluşları ile bilgi alışverişini sağlar.
Yükümlülük	• Siber Güvenlik Stratejisi • Siber Güvenlik Politikası
Ana görevler)	• Kurumsal hedefleri desteklemek için iş stratejisiyle uyumlu siber güvenlik hedeflerini, gereksinimleri, stratejileri, politikaları tanımlayın, uygulayın, iletin ve sürdürün • Kuruluşun üst yönetimi tarafından onaylanmak üzere siber güvenlik vizyonu, stratejileri ve politikaları hazırlamak ve sunmak ve bunların yürütülmesini sağlamak • Bilgi Güvenliği Yönetiminin uygulanmasını ve geliştirilmesini denetlemek Sistem (BGYS) • Üst yönetimi siber güvenlik riskleri, tehditler ve bunların kuruluşa etkileri konusunda eğitin • Üst yönetimin kuruluşun siber güvenlik risklerini onaylamasını sağlayın • Siber güvenlik planları geliştirin • Siber güvenlikle ilgili yetkililer ve topluluklarla ilişkiler geliştirin • Siber güvenlik olaylarını, riskleri ve bulguları üst yönetime bildirin • Siber güvenlikteki ilerlemeyi izleyin • Siber güvenlik stratejisini uygulamak için kaynakları güvenli hale getirin • Üst yönetimle siber güvenlik bütçesini görüşün • Kuruluşun siber olaylara karşı dayanıklılığını sağlamak • Kuruluş içinde sürekli kapasite geliştirmeyi yönetin • Uygun siber güvenlik kaynaklarını gözden geçirin, planlayın ve tahsis edin

Anahtar beceriler)	• Bir kuruluşun siber güvenlik duruşunu değerlendirin ve geliştirin • Siber güvenlik politikalarını, sertifikaları, standartları, metodolojileri ve çerçeveleri analiz edin ve uygulayın • Siber güvenlikle ilgili yasa, yönetmelik ve mevzuatları analiz edin ve bunlara uyun • Siber güvenlik önerilerini ve en iyi uygulamaları uygulayın • Siber güvenlik kaynaklarını yönetin • Bir siber güvenlik stratejisinin geliştirilmesi, desteklenmesi ve yürütülmesine liderlik etmek • Bir kuruluşun siber güvenlik kültürünü etkileyin • Bilgi Güvenliği Yönetim Sistemini (BGYS) doğrudan veya dış kaynak kullanımına yönlendirerek tasarlayın, uygulayın, izleyin ve gözden geçirin • Güvenlik belgelerini, raporları, SLA'ları gözden geçirin ve geliştirin ve güvenlik hedeflerini sağlayın • Siber güvenlikle ilgili sorunları belirleyin ve çözün • Bir siber güvenlik planı oluşturun • İç ve dış paydaşlarla iletişim kurmak, koordine etmek ve işbirliği yapmak • Kuruluşun bilgi güvenliği stratejisinde gerekli değişiklikleri tahmin edin ve yeni planlar formüle edin	
	• Siber güvenlik yönetimi için olgunluk modellerini tanımlayın ve uygulayın • Siber güvenlik tehditlerini, ihtiyaçlarını ve yaklaşan zorlukları tahmin edin • İnsanları motive edin ve teşvik edin	
Anahtar bilgi	• Siber güvenlik politikaları • Siber güvenlik standartları, metodolojileri ve çerçeveleri • Siber güvenlik önerileri ve en iyi uygulamalar • Siber güvenlikle ilgili yasa, yönetmelik ve mevzuatlar • Siber güvenlikle ilgili sertifikalar • Etik siber güvenlik organizasyonu gereksinimleri • Siber güvenlik olgunluk modelleri • Siber güvenlik prosedürleri • Kaynak yönetimi • Yönetim Uygulamaları • Risk yönetimi standartları, metodolojileri ve çerçeveleri	
e-Yetkinlikler (e-CF'den)	A.7. Teknoloji Trend İzleme D.1. Bilgi Güvenliği Stratejisi Geliştirme E.3. Risk yönetimi E.8. Bilgi Güvenliği Yönetimi E.9. IS-Yönetişim	Seviye 4 Seviye 5 Seviye 4 Seviye 4 Seviye 5

2.2 SİBER OLAY MÜDAHALECİ

Profil başlığı	Siber Olay Müdahalecisi
Alternatif Başlık(lar)	Siber Olay İşleyicisi Siber Kriz Uzmanı Olay Müdahale Mühendisi Güvenlik Operasyonları Merkezi (SOC) Analisti Siber Savaşçı / Savunmacı Güvenlik Operasyon Analisti (SOC Analisti) Siber Güvenlik SIEM Yöneticisi
Özet beyanı	Kuruluşun siber güvenlik durumunu izleyin, siber saldırılar sırasında olayları ele alın ve ICT sistemlerinin devam etmesini sağlayın.
Misyon	Sistemlerin siber güvenlik durumunu izler ve değerlendirir. Siber güvenlik olaylarının etkisini analiz eder, değerlendirir ve azaltır. Siber olayların kök nedenlerini ve kötü niyetli aktörleri tanımlar. Kuruluşun Olay Müdahale Planına göre, kanıtları toplayarak ve alınan eylemleri belgeleyerek sistemlerin ve süreçlerin işlevselliklerini çalışır duruma getirir.
Yükümlülük	• Olay Müdahale Planı • Siber Olay Raporu
Ana görevler)	• Olayın geliştirilmesine, sürdürülmesine ve değerlendirilmesine katkıda bulunmak Müdahale Planı • Olay işleme ile ilgili prosedürleri geliştirmek, uygulamak ve değerlendirmek • Siber güvenlik olaylarını tanımlayın, analiz edin, azaltın ve iletin • Teknik güvenlik açıklarını değerlendirin ve yönetin • Siber güvenlik olaylarını algılama ve müdahale etkinliğini ölçün • Bir siber güvenlik veya veri ihlali olayından sonra gerçekleştirilen siber güvenlik kontrollerinin ve azaltma eylemlerinin esnekliğini değerlendirin • Olay işleme test tekniklerini benimseyin ve geliştirin • Olay sonuçları analizi ve olay işleme raporlaması için prosedürler oluşturun • Olay sonuçları analizini ve olay işleme eylemlerini belgeleyin • Güvenli Operasyon Merkezleri (SOC'ler) ve Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT'ler) ile işbirliği yapın • Güvenlik olaylarının geçerli yasal çerçeveye göre raporlanması için kilit personel ile işbirliği yapın
Anahtar beceriler)	• Siber güvenlik olaylarının ele alınması ve müdahalesinin tüm teknik, işlevsel ve operasyonel yönlerini uygulayın • Birden çok kaynaktan gelen siber tehdit bilgilerini toplayın, analiz edin ve ilişkilendirin • İşletim sistemleri, sunucular, bulutlar ve ilgili altyapılar üzerinde çalışın • Baskı altında çalışmak • İlgili paydaşlarla iletişim kurun, sunun ve raporlayın • Günlük dosyalarını yönetin ve analiz edin
Anahtar bilgi	• Olay işleme standartları, metodolojileri ve çerçeveleri • Olay işleme önerileri ve en iyi uygulamalar • Olay işleme araçları • Olay işleme iletişim prosedürleri • İşletim sistemleri güvenliği • Bilgisayar ağları güvenliği • Siber tehditler • Siber güvenlik saldırı prosedürleri • Bilgisayar sistemleri güvenlik açıkları • Siber güvenlikle ilgili sertifikalar • Siber güvenlikle ilgili yasa, yönetmelik ve mevzuatlar • Güvenli Operasyon Merkezleri (SOC'ler) operasyonu

	• Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT'ler) operasyonu	
e-Yetkinlikler (e-CF'den)	A.7. Teknoloji Trend İzleme B.2. Bileşen Entegrasyonu	3. seviye Seviye 2
	B.3. Test yapmak B.5. Dokümantasyon Üretimi C.4. Sorun Yönetimi	3. seviye 3. seviye Seviye 4

2.3 SİBER HUKUKİ, POLİTİKA VE UYUM MEMURU

Profil başlığı	Siber Hukuk, Politika ve Uyum Görevlisi
Alternatif Başlık(lar)	Veri Koruma Görevlisi (DPO) Gizlilik Koruma Görevlisi Siber Hukuk Danışmanı Siber Hukuk Danışmanı Bilgi Yönetim Görevlisi Veri Uyum Görevlisi Siber Güvenlik Hukuk Görevlisi BT/BİT Uyum Yöneticisi Yönetişim Risk Uyumluluğu (GRC) Danışmanı
Özet beyanı	Kuruluşun stratejisine ve yasal gereksinimlerine dayalı olarak siber güvenlikle ilgili standartlar, yasal ve düzenleyici çerçevelerle uyumluluğu yönetir.
Misyon	Kuruluşun stratejisi ve yasal gereksinimleri doğrultusunda siber güvenlik ve verilerle ilgili yasal, düzenleyici çerçeveler ve politikalarla uyumluluğu denetler ve sağlar. Kuruluşun veri korumayla ilgili eylemlerine katkıda bulunur. Uyumluluğu sağlamak için kuruluşun siber güvenlik yönetişim süreçlerinin ve önerilen iyileştirme stratejilerinin/çözümlerinin geliştirilmesinde yasal tavsiye sağlar.
Yükümlülük	• Uyumluluk Kılavuzu • Uyumluluk raporu
Ana görevler)	• Veri gizliliği ve veri koruma standartları, yasaları ve yönetmeliklerine uygunluğu sağlayın ve bunlarla ilgili yasal tavsiye ve rehberlik sağlayın • Uyumluluk boşluklarını belirleyin ve belgeleyin • Gizlilik etki değerlendirmeleri yapın ve gizlilik politikaları, prosedürleri geliştirin, sürdürün, iletin ve eğitin • Kuruluşun veri gizliliği ve koruma programını uygulamak ve savunmak • Veri sahiplerinin, sahiplerinin, kontrolörlerin, işlemcilerin, öznelerin, dahili veya harici ortakların ve kuruluşların veri koruma hakları, yükümlülükleri ve sorumlulukları hakkında bilgilendirilmesini sağlamak • Veri işlemeyle ilgili soru ve şikayetleri ele almak için önemli bir iletişim noktası olarak hareket edin • Siber güvenlik ve gizlilik uyumluluğunu sağlamak için tasarlama, uygulama, denetleme ve uyumluluk testi etkinliklerine yardımcı olun • Denetimleri ve veri korumayla ilgili eğitim faaliyetlerini izleyin • Yetkililer ve profesyonel gruplarla işbirliği yapın ve bilgi paylaşın • Kuruluşun siber güvenlik stratejisi, politikası ve prosedürlerinin geliştirilmesine katkıda bulunmak • Uyumluluğu sağlamak ve kuruluş içinde bir veri koruma kültürünü teşvik etmek için personel bilinçlendirme eğitimi geliştirin ve önerin • Bilgi güvenliği sorumluluklarının ve üçüncü taraf ilişkilerinin yasal yönlerini yönetin

Anahtar beceriler)	• İş stratejisi, modelleri ve ürünleri hakkında kapsamlı bir anlayış ve yasal, düzenleyici ve standartların gerekliliklerini hesaba katma becerisi • Kurumsal süreçlerin, finans ve iş stratejisinin uygulanmasında yer alan veri koruma ve gizlilik konularının çalışma hayatı uygulamalarını yürütmek • İş ihtiyaçlarını ve yasal gereklilikleri tamamlayan uygun siber güvenlik ve gizlilik politikaları ve prosedürlerinin geliştirilmesine öncülük etmek; ayrıca kabulünü, anlaşılmasını ve uygulanmasını sağlamak ve ilgili taraflar arasında iletmek • Standartları, çerçeveleri, kabul edilen metodolojileri ve araçları kullanarak gizlilik etki değerlendirmelerini yürütün, izleyin ve gözden geçirin • Paydaşlara ve kullanıcılara veri koruma ve gizlilik konularını açıklayın ve iletin • Etik gereklilikleri ve standartları anlamak, uygulamak ve bunlara uymak • Yasal çerçeve değişikliklerinin kuruluşun siber güvenlik ve veri koruma stratejisi ve politikaları üzerindeki etkilerini anlayın • Diğer ekip üyeleri ve meslektaşları ile işbirliği yapın	
Anahtar bilgi	• Siber güvenlikle ilgili yasa, yönetmelik ve mevzuatlar	
	• Siber güvenlik standartları, metodolojileri ve çerçeveleri • Siber güvenlik politikaları • Yasal, düzenleyici ve yasal uyumluluk gereksinimleri, öneriler ve en iyi uygulamalar • Gizlilik etki değerlendirme standartları, metodolojileri ve çerçeveleri	
e-Yetkinlikler (e-CF'den)	A.1. Bilgi Sistemleri ve İş Stratejisi hizalama D.1. Bilgi Güvenliği Stratejisi Geliştirme E.8. Bilgi Güvenliği Yönetimi E.9. IS-Yönetişim	Seviye 4 Seviye 4 3. seviye Seviye 4

2.4 SİBER TEHDİT İSTİHBARAT UZMANI

Profil başlığı	Siber Tehdit İstihbarat Uzmanı
Alternatif Başlık(lar)	Siber İstihbarat Analisti Siber Tehdit Modelleyici
Özet beyanı	Eyleme geçirilebilir istihbarat raporları üretmek ve bunları hedef paydaşlara yaymak için veri ve bilgileri toplayın, işleyin, analiz edin.
Misyon	Siber tehdit bilgilerinin toplanması, analiz edilmesi ve eyleme geçirilebilir istihbaratın üretilmesi ve güvenlik paydaşlarına ve CTI topluluğuna taktik, operasyonel ve stratejik düzeyde yayılması dahil siber tehdit istihbarat yaşam döngüsünü yönetir. Siber tehdit aktörleri tarafından kullanılan Taktikler, Teknikler ve Prosedürleri (TTP'ler) ve bunların eğilimlerini belirler ve izler, tehdit aktörlerinin faaliyetlerini takip eder ve siber olmayan olayların siber bağlantılı eylemleri nasıl etkileyebileceğini gözlemler.
Yükümlülük	• Siber Tehdit İstihbaratı Kılavuzu • Siber Tehdit Raporu
Ana görevler)	• Kuruluşun siber tehdit istihbarat stratejisini geliştirmek, uygulamak ve yönetmek • Tehdit istihbaratını yönetmek için planlar ve prosedürler geliştirin • İş gereksinimlerini İstihbarat Gereksinimlerine çevirin • Tehdit istihbaratı toplama, analiz etme ve eyleme geçirilebilir istihbarat üretme ve güvenlik paydaşlarına yayma uygulama • Kuruluşu hedef alan siber tehdit aktörlerini belirleyin ve değerlendirin • Açık kaynaklı ve özel verileri, bilgileri ve istihbaratı analiz ederek siber tehdit aktörleri tarafından kullanılan Taktikler, Teknikler ve Prosedürleri (TTP'ler) belirleyin, izleyin ve değerlendirin • Tehdit istihbaratı verilerine dayalı olarak eyleme dönüştürülebilir raporlar üretin • Taktik, operasyonel ve stratejik düzeyde azaltma planlarını detaylandırın ve tavsiyede bulunun • İlgili siber tehditler hakkında istihbarat paylaşmak ve tüketmek için paydaşlarla koordinasyon sağlayın • Tehdit modelleme, Risk Azaltma ve siber tehdit avcılığı için tavsiyeleri desteklemek ve yardımcı olmak için istihbarat verilerinden yararlanın • İstihbaratı her düzeyde açıkça ve kamuya açıklayın ve iletin • Riske maruz kalmayı ve bunun sonuçlarını teknik olmayan paydaşlara açıklayarak uygun güvenlik ciddiyetini iletin
Anahtar beceriler)	• Diğer ekip üyeleri ve meslektaşları ile işbirliği yapın • Birden çok kaynaktan gelen siber tehdit bilgilerini toplayın, analiz edin ve ilişkilendirin • Tehdit aktörlerinin TTP'lerini ve kampanyalarını belirleyin • Tehdit istihbaratı yönetim prosedürlerini otomatikleştirin • Teknik analiz ve raporlama yapmak • Siber ile ilgili faaliyetler üzerinde etkileri olan siber olmayan olayları tanımlayın • Tehditleri, aktörleri ve TTP'leri modelleyin • İç ve dış paydaşlarla iletişim kurmak, koordine etmek ve işbirliği yapmak • İlgili paydaşlarla iletişim kurmak, sunmak ve raporlamak • CTI platformlarını ve araçlarını kullanın ve uygulayın

Anahtar bilgi	• İşletim sistemleri güvenliği • Bilgisayar ağları güvenliği • Siber güvenlik kontrolleri ve çözümleri • Bilgisayar Programlama • Siber Tehdit İstihbaratı (CTI) paylaşım standartları, metodolojileri ve çerçeveleri • Sorumlu bilgi ifşa prosedürleri • Siber güvenlikle ilgili etki alanları arası ve etki alanları arası bilgi • Siber tehditler • Siber tehdit aktörleri • Siber güvenlik saldırı prosedürleri • Gelişmiş ve kalıcı siber tehditler (APT) • Tehdit aktörleri Taktikler, Teknikler ve Prosedürler (TTP'ler) • Siber güvenlikle ilgili sertifikalar	
e-Yetkinlikler (e-CF'den)	B.5. Dokümantasyon Üretimi D.7. Veri Bilimi ve Analitiği D.10. Bilgi ve Bilgi Yönetimi E 4. İlişkileri yönetimi E.8. Bilgi Güvenliği Yönetimi	3. seviye Seviye 4 Seviye 4 3. seviye Seviye 4

2.5 SİBER GÜVENLİK MİMARİ

Profil başlığı	Siber Güvenlik Mimarı
Alternatif Başlık(lar)	Siber Güvenlik Çözümleri Mimarı Siber Güvenlik Tasarımcısı Veri Güvenliği Mimarı
Özet beyanı	Tasarıma dayalı güvenlik çözümleri (altyapılar, sistemler, varlıklar, yazılım, donanım ve hizmetler) ve siber güvenlik kontrollerini planlar ve tasarlar.
Misyon	Tasarım gereği güvenlik ve tasarım gereği gizlilik ilkelerine dayalı çözümler tasarlar. Mimari modeller oluşturur ve sürekli olarak geliştirir ve uygun mimari dokümantasyon ve spesifikasyonlar geliştirir. Standartlar ve diğer ilgili gereksinimler doğrultusunda siber güvenlik bileşenlerinin güvenli geliştirmesini, entegrasyonunu ve bakımını koordine edin.
Yükümlülük	• Siber Güvenlik Mimarisi Şeması • Siber Güvenlik Gereksinimleri Raporu
Ana görevler)	• Kuruluşun stratejisini uygulamak için güvenli bir mimari tasarlayın ve önerin • Güvenlik ve gizlilik gereksinimlerini karşılamak için kuruluşun siber güvenlik mimarisini geliştirin • Mimari dokümantasyon ve spesifikasyonlar üretin • Paydaşlara üst düzey güvenlik mimarisi tasarımı sunun • Sistemlerin, hizmetlerin ve ürünlerin geliştirme yaşam döngüsü boyunca güvenli bir ortam oluşturun • Siber güvenlik özelliklerini sağlayan siber güvenlik bileşenlerinin geliştirilmesini, entegrasyonunu ve bakımını koordine etmek • Kuruluş mimarisinin siber güvenliğini analiz edin ve değerlendirin • Güvenlik incelemeleri ve sertifikalandırma yoluyla çözüm mimarilerinin güvenliğini sağlayın • Diğer ekipler ve iş arkadaşlarıyla işbirliği yapın • Siber güvenlik çözümlerinin kuruluşun mimarisinin tasarımı ve performansı üzerindeki etkisini değerlendirin • Kuruluşun mimarisini ortaya çıkan tehditlere göre uyarlayın • Uygun bir güvenlik düzeyini korumak için uygulanan mimariyi değerlendirin
Anahtar beceriler)	• Kullanıcı ve iş güvenliği gereksinimleri analizi yapmak • Siber güvenlik mimari ve işlevsel özelliklerini çizin • Güvenlik ve gizlilik gereksinimlerini geliştirmek ve etkili çözümleri belirlemek için sistemleri ayrıştırın ve analiz edin • Tasarım gereği güvenlik ve mahremiyete ve varsayılan olarak siber güvenlik ilkelerine dayalı tasarım sistemleri ve mimarileri • Uygulayıcılar ve BT/OT personeline rehberlik edin ve onlarla iletişim kurun • İlgili paydaşlarla iletişim kurmak, sunmak ve raporlamak • Paydaşların ihtiyaçlarına ve bütçesine dayalı siber güvenlik mimarileri önermek • Uygun özellikleri, prosedürleri ve kontrolleri seçin • Mimari genelinde başarısızlık noktalarına karşı dayanıklılık oluşturun • Güvenlik çözümlerinin entegrasyonunu koordine edin

Anahtar bilgi	• Siber güvenlikle ilgili sertifikalar • Siber güvenlik önerileri ve en iyi uygulamalar • Siber güvenlik standartları, metodolojileri ve çerçeveleri • Siber güvenlikle ilgili gereksinim analizi • Güvenli geliştirme yaşam döngüsü • Güvenlik mimarisi referans modelleri • Siber güvenlikle ilgili teknolojiler • Siber güvenlik kontrolleri ve çözümleri • Siber güvenlik riskleri • Siber tehditler • Siber güvenlik trendleri • Yasal, düzenleyici ve yasal uyumluluk gereksinimleri, öneriler ve en iyi uygulamalar • Eski siber güvenlik prosedürleri • Gizlilik Artırıcı Teknolojiler (PET)	
	• Tasarıma göre gizlilik standartları, metodolojileri ve çerçeveleri	
e-Yetkinlikler (e-CF'den)	A.5. Mimari tasarım A.6. Uygulama Tasarımı B.1. Uygulama geliştirme B.3. Test yapmak B.6. BİT Sistemleri Mühendisliği	Seviye 5 3. seviye 3. seviye 3. seviye Seviye 4

2.6 SİBER GÜVENLİK DENETÇİSİ

Profil başlığı	Siber Güvenlik Denetçisi
Alternatif Başlık(lar)	Bilgi Güvenliği Denetçisi (BT veya Hukuk Denetçisi) Yönetişim Risk Uyum (GRC) Denetçisi Siber Güvenlik Denetim Müdürü Siber Güvenlik Prosedür ve Süreçleri Denetçisi Bilgi Güvenliği Riski ve Uyum Denetçisi Veri Koruma Değerlendirme Analisti
Özet beyanı	Kuruluşun ekosisteminde siber güvenlik denetimleri gerçekleştirin. Yasal, düzenleyici, politika bilgileri, güvenlik gereksinimleri, endüstri standartları ve en iyi uygulamalara uygunluğun sağlanması.
Misyon	Süreçlerin ve kontrollerin etkinliğini ve kuruluşun yasal ve düzenleyici çerçeve politikalarıyla genel uyumluluğunu değerlendirmek için bağımsız incelemeler yapar. Siber güvenlikle ilgili ürünleri (sistemler, donanım, yazılım ve hizmetler), yönergelere, standartlara ve düzenlemelere uygunluğu sağlayan işlev ve politikaları değerlendirir, test eder ve doğrular.
Yükümlülük	• Siber Güvenlik Denetim Planı • Siber Güvenlik Denetim Raporu
Ana görevler)	• Kuruluşun denetim politikasını, prosedürlerini, standartlarını ve yönergelerini geliştirmek • Sistem denetimi için kullanılan metodolojileri ve uygulamaları oluşturun • Hedef ortamı oluşturmak ve denetim faaliyetlerini yönetmek • Denetim kapsamını, amaçlarını ve denetim kriterlerini tanımlayın • Çerçeveleri, standartları, metodolojiyi, prosedürleri ve denetim testlerini açıklayan bir denetim planı geliştirin • Risk profiline dayalı olarak değerlendirme hedefini, güvenlik hedeflerini ve gereksinimleri gözden geçirin • Siber güvenlikle ilgili geçerli yasa ve yönetmeliklere uygunluğu denetleyin • Siber güvenlikle ilgili geçerli standartlara uygunluğu denetleyin • Denetim planını yürütün ve kanıtları ve ölçümleri toplayın • Denetim kayıtlarının bütünlüğünü korumak ve korumak • Uygunluk değerlendirmesi, güvence, denetim, belgelendirme ve bakım raporları geliştirmek ve iletmek • Risk iyileştirme faaliyetlerini izleyin
Anahtar beceriler)	• Kanıtlara dayalı sistematik ve deterministik bir şekilde organize olun ve çalışın • Denetim çerçevelerini, standartlarını ve metodolojilerini takip edin ve uygulayın • Denetim araçlarını ve tekniklerini uygulamak • İş süreçlerini analiz edin, yazılım veya donanım güvenliğini ve ayrıca teknik ve organizasyonel kontrolleri değerlendirin ve gözden geçirin • Zayıflıkları ve etkisiz kontrolleri belirlemek için sistemleri ayrıştırın ve analiz edin • Yasal ve düzenleyici gereksinimleri ve iş ihtiyaçlarını iletin, açıklayın ve uyarlayın • Denetim bilgilerini toplamak, değerlendirmek, sürdürmek ve korumak • Dürüst, tarafsız ve bağımsız denetim

Anahtar bilgi	• Siber güvenlik kontrolleri ve çözümleri • Yasal, düzenleyici ve yasal uyumluluk gereksinimleri, öneriler ve en iyi uygulamalar • Siber güvenlik kontrollerinin etkinliğini izleme, test etme ve değerlendirme • Uygunluk değerlendirme standartları, metodolojileri ve çerçeveleri • Denetim standartları, metodolojileri ve çerçeveleri • Siber güvenlik standartları, metodolojileri ve çerçeveleri • Denetimle ilgili sertifikasyon • Siber güvenlikle ilgili sertifikalar	
e-Yetkinlikler (e-CF'den)	B.3. Test yapmak B.5. Dokümantasyon Üretimi E.3. Risk yönetimi E.6 BİT Kalite Yönetimi	Seviye 4 3. seviye Seviye 4 Seviye 4
	E.8. Bilgi Güvenliği Yönetimi	Seviye 4

2.7 SİBER GÜVENLİK EĞİTMENİ

Profil başlığı	Siber Güvenlik Eğitimcisi	
Alternatif Başlık(lar)	Siber Güvenlik Farkındalık Uzmanı Siber Güvenlik Eğitmeni Siber Güvenlik Fakültesi (Profesör, Öğretim Üyesi)	
Özet beyanı	İnsanların siber güvenlik bilgi, beceri ve yetkinliklerini geliştirir.	
Misyon	Siber güvenlik ve veri koruma ile ilgili konularda farkındalık, eğitim ve eğitim programları tasarlar, geliştirir ve yürütür. İnsan kaynaklarının siber güvenlik kültürünü, yeteneklerini, bilgi ve becerilerini iletmek ve geliştirmek için uygun öğretim ve eğitim yöntemlerini, tekniklerini ve araçlarını kullanır. Siber güvenliğin önemini teşvik eder ve onu kuruluşta birleştirir.	
Yükümlülük	• Siber Güvenlik Farkındalık Programı • Siber Güvenlik Eğitim Materyali	
Ana görevler)	• İçerik, yöntem, araçlar ve kursiyerlerin ihtiyaçlarına göre eğitim ve farkındalık için siber güvenlik ve veri koruma müfredatı ve eğitim materyali geliştirmek, güncellemek ve sunmak • Siber güvenlik ve veri koruma farkındalığı artırma faaliyetleri, seminerler, kurslar, uygulamalı eğitimler düzenleyin, tasarlayın ve sunun • Eğitim etkinliğini izlemek, değerlendirmek ve raporlamak • Stajyerin performansını değerlendirin ve raporlayın • Eğitim, öğretim ve bilinçlendirme için yeni yaklaşımlar bulmak • Siber güvenlik simülasyonları, sanal laboratuvarlar veya siber menzil ortamları tasarlayın, geliştirin ve sunun • Bireyler için siber güvenlik sertifika programları hakkında rehberlik sağlayın • Uzmanlığı sürekli olarak sürdürmek ve geliştirmek; Siber güvenlik kapasitelerinin ve yeteneklerinin sürekli olarak geliştirilmesini teşvik etmek ve güçlendirmek	
Anahtar beceriler)	• Siber güvenlik farkındalığı, eğitimi ve öğretimindeki ihtiyaçları belirleyin • Siber güvenlik ihtiyaçlarını karşılamak için öğrenme programları tasarlayın, geliştirin ve sunun • Siber menzil ortamlarını kullanan simülasyonlar dahil siber güvenlik alıştırmaları geliştirin • Siber güvenlik ve veri koruma profesyonel sertifikalarına yönelik eğitim sağlayın • Siber güvenlikle ilgili mevcut eğitim kaynaklarını kullanın • Farkındalık, eğitim ve öğretim faaliyetleri için değerlendirme programları geliştirmek • İlgili paydaşlarla iletişim kurmak, sunmak ve raporlamak • Hedef kitle için uygun pedagojik yaklaşımları belirleyin ve seçin • İnsanları motive edin ve teşvik edin	
Anahtar bilgi	• Pedagojik standartlar, metodolojiler ve çerçeveler • Siber güvenlik bilinci, eğitim ve öğretim programı geliştirme • Siber güvenlikle ilgili sertifikalar • Siber güvenlik eğitim ve öğretim standartları, metodolojileri ve çerçeveleri • Siber güvenlikle ilgili yasa, yönetmelik ve mevzuatlar • Siber güvenlik önerileri ve en iyi uygulamalar • Siber güvenlik standartları, metodolojileri ve çerçeveleri • Siber güvenlik kontrolleri ve çözümleri	
e-Yetkinlikler (e-CF'den)	D.3. Eğitim ve Öğretim Temini D.9. Personel Gelişimi E.8. Bilgi Güvenliği Yönetimi	3. seviye 3. seviye 3. seviye

2.8 SİBER GÜVENLİK UYGULAYICI

Profil başlığı	Siber Güvenlik Uygulayıcı
Alternatif Başlık(lar)	Bilgi Güvenliği Uygulayıcı Siber Güvenlik Çözümleri Uzmanı Siber Güvenlik Geliştiricisi Siber Güvenlik Mühendisi Geliştirme, Güvenlik ve Operasyonlar (DevSecOps) Mühendisi
Özet beyanı	Altyapılar ve ürünler üzerinde siber güvenlik çözümleri (sistemler, varlıklar, yazılımlar, kontroller ve hizmetler) geliştirin, dağıtın ve çalıştırın.
Misyon	Siber güvenlikle ilgili teknik geliştirme, entegrasyon, test etme, uygulama, çalıştırma, bakım, izleme ve siber güvenlik çözümlerinin desteklenmesini sağlar. Spesifikasyonlara ve uygunluk gereksinimlerine bağlılığı sağlar, sağlam performansı garanti eder ve şartnamede gerekli olan teknik sorunları çözer. kuruluşun siber güvenlikle ilgili çözümleri (sistemler, varlıklar, yazılımlar, kontroller ve hizmetler), altyapılar ve ürünler.
Yükümlülük	• Siber Güvenlik Çözümleri
Ana görevler)	• Siber güvenlik ürünlerini geliştirin, uygulayın, bakımını yapın, yükseltin, test edin • Kullanıcılara ve müşterilere siber güvenlikle ilgili destek sağlayın • Siber güvenlik çözümlerini entegre edin ve sorunsuz çalışmasını sağlayın • Sistemleri, hizmetleri ve ürünleri güvenli bir şekilde yapılandırın • Sistemlerin, hizmetlerin ve ürünlerin güvenliğini korumak ve yükseltmek • Siber güvenlik prosedürlerini ve kontrollerini uygulayın • Uygulanan siber güvenlik kontrollerinin performansını izleyin ve sağlayın • Sistemlerin, hizmetlerin ve ürünlerin güvenliğini belgeleyin ve raporlayın • Siber güvenlikle ilgili eylemlerde BT/OT personeliyle yakın çalışın • Teknik güvenlik açıklarını gidermek için ürünlere yamalar uygulayın, uygulayın ve yönetin
Anahtar beceriler)	• İlgili paydaşlarla iletişim kurmak, sunmak ve raporlamak • Siber güvenlik çözümlerini kuruluşun altyapısına entegre edin • Çözümleri kuruluşun güvenlik politikasına göre yapılandırın • Çözümlerin güvenliğini ve performansını değerlendirin • Kod, komut dosyaları ve programlar geliştirin • Siber güvenlikle ilgili sorunları belirleyin ve çözün • Diğer ekip üyeleri ve meslektaşları ile işbirliği yapın
Anahtar bilgi	• Güvenli geliştirme yaşam döngüsü • Bilgisayar Programlama • İşletim sistemleri güvenliği • Bilgisayar ağları güvenliği • Siber güvenlik kontrolleri ve çözümleri • Saldırgan ve defansif güvenlik uygulamaları • Güvenli kodlama önerileri ve en iyi uygulamalar • Siber güvenlik önerileri ve en iyi uygulamalar • Standartları, metodolojileri ve çerçeveleri test etme • Test prosedürleri • Siber güvenlikle ilgili teknolojiler

e-Yetkinlikler (e-CF'den)	A.5. Mimari tasarım A.6. Uygulama Tasarımı B.1. Uygulama geliştirme B.3. Test yapmak B.6. BİT Sistemleri Mühendisliği	3. seviye 3. seviye 3. seviye 3. seviye Seviye 4

2.9 SİBER GÜVENLİK ARAŞTIRMACI

Profil başlığı	Siber Güvenlik Araştırmacısı
Alternatif Başlık(lar)	Siber Güvenlik Araştırma Mühendisi Siber güvenlikte Baş Araştırma Görevlisi (CRO) Siber güvenlikte Kıdemli Araştırma Görevlisi Siber güvenlikte Araştırma ve Geliştirme (Ar-Ge) Görevlisi Siber güvenlikte Bilimsel Kadro Siber güvenlikte Araştırma ve İnovasyon Sorumlusu/Uzmanı Siber güvenlik alanında araştırma görevlisi
Özet beyanı	Siber güvenlik alanını araştırın ve sonuçları siber güvenlik çözümlerine dahil edin.
Misyon	Temel/temel ve uygulamalı araştırmalar yürütür ve diğer paydaşlarla işbirliği yaparak siber güvenlik alanında yeniliği kolaylaştırır. Siber güvenlikteki eğilimleri ve bilimsel bulguları analiz eder.
Yükümlülük	• Siber Güvenlikte Yayın
Ana görevler)	• Siber güvenlik teknolojilerini, çözümlerini, gelişmelerini ve süreçlerini analiz edin ve değerlendirin • Siber güvenlikle ilgili konularda araştırma, yenilik ve geliştirme çalışmaları yürütün• Araştırma ve yenilik fikirleri ortaya koyun ve üretin • Siber güvenlikle ilgili konularda en son teknolojiyi geliştirin • Yenilikçi siber güvenlikle ilgili çözümlerin geliştirilmesine yardımcı olun • Siber güvenlik çözümleri için deneyler yapın ve konsept kanıtı, pilot uygulamalar ve prototipler geliştirin • Projeleri desteklemek için bir kavram kanıtı oluşturma ve test etme dahil çerçeveler, yöntemler, standartlar, araçlar ve protokolleri seçin ve uygulayın • En son siber güvenlik iş fikirlerine, hizmetlerine ve çözümlerine katkıda bulunur • Farkındalık, teorik eğitim, pratik eğitim, test etme, danışmanlık, denetleme ve paylaşma dahil olmak üzere siber güvenlikle ilgili kapasite geliştirmeye yardımcı olun • Sektörler arası siber güvenlik başarılarını belirleyin ve bunları farklı bir bağlamda uygulayın veya yenilikçi yaklaşımlar ve çözümler önerin • Proje yönetimi ve bütçeleme dahil olmak üzere inovasyon süreçlerine ve projelerine liderlik etmek veya katılmak • Bilimsel çalışmaları ve araştırma ve geliştirme sonuçlarını yayınlamak ve sunmak
Anahtar beceriler)	• Yeni fikirler üretin ve teoriyi pratiğe aktarın • Zayıflıkları ve etkisiz kontrolleri belirlemek için sistemleri ayrıştırın ve analiz edin • Güvenlik ve gizlilik gereksinimlerini geliştirmek ve etkili çözümleri belirlemek için sistemleri ayrıştırın ve analiz edin • Siber güvenlikle ilgili teknolojilerdeki yeni gelişmeleri izleyin • İlgili paydaşlarla iletişim kurmak, sunmak ve raporlamak • Siber güvenlikle ilgili sorunları belirleyin ve çözün • Diğer ekip üyeleri ve meslektaşları ile işbirliği yapın

Anahtar bilgi	• Siber güvenlikle ilgili araştırma, geliştirme ve yenilik (RDI) • Siber güvenlik standartları, metodolojileri ve çerçeveleri • Siber güvenlikle ilgili teknolojilerin serbest bırakılması veya kullanılmasına ilişkin yasal, düzenleyici ve yasal gereklilikler • Siber güvenliğin çok disiplinli yönü • Sorumlu bilgi ifşa prosedürleri	
e-Yetkinlikler (e-CF'den)	A.7. Teknoloji Trend İzleme A.9. yenilik D.7. Veri Bilimi ve Analitiği C.4. Sorun Yönetimi D.10. Bilgi ve Bilgi Yönetimi	Seviye 5 Seviye 5 Seviye 4 3. seviye 3. seviye

2.10 SİBER GÜVENLİK RİSK MÜDÜRÜ

Profil başlığı	**Siber Güvenlik Risk Yöneticisi**
Alternatif Başlık(lar)	Bilgi Güvenliği Risk Analisti Siber Güvenlik Risk Güvencesi Danışmanı Siber Güvenlik Risk Değerlendiricisi Siber Güvenlik Etki Analisti Siber Risk Yöneticisi
Özet beyanı	Kuruluşun stratejisiyle uyumlu siber güvenlikle ilgili riskleri yönetin. Risk yönetimi süreçlerini ve raporlarını geliştirin, sürdürün ve iletin.
Misyon	Risk analizi, değerlendirmesi ve tedavisini planlayarak, uygulayarak, raporlayarak ve ileterek BİT altyapılarının, sistemlerinin ve hizmetlerinin siber güvenlikle ilgili risklerini sürekli olarak yönetir (tanımlar, analiz eder, değerlendirir, tahmin eder, azaltır). Kuruluş için bir risk yönetimi stratejisi oluşturur ve hafifletme eylemlerini ve kontrollerini seçerek risklerin kuruluş için kabul edilebilir bir seviyede kalmasını sağlar.
Yükümlülük	• Siber Güvenlik Risk Değerlendirme Raporu • Siber Güvenlik Risk İyileştirme Eylem Planı
Ana görevler)	• Bir kuruluşun siber güvenlik risk yönetimi stratejisini geliştirin • Kuruluşun varlıklarının bir envanterini yönetin • BİT sistemlerinin siber güvenlikle ilgili tehditlerini ve güvenlik açıklarını belirleyin ve değerlendirin • Saldırganların profillerini ve saldırıların potansiyelinin tahminini içeren tehdit ortamının belirlenmesi • Siber güvenlik risklerini değerlendirin ve kuruluşun stratejisine en iyi şekilde hitap eden güvenlik kontrolleri ve risk azaltma ve kaçınma dahil olmak üzere en uygun risk işleme seçeneklerini önerin • Siber güvenlik kontrollerinin ve risk seviyelerinin etkinliğini izleyin • Tüm siber güvenlik risklerinin kuruluşun varlıkları için kabul edilebilir bir seviyede kalmasını sağlayın • Eksiksiz bir risk yönetimi döngüsü geliştirin, sürdürün, raporlayın ve iletin
Anahtar beceriler)	• Siber güvenlik risk yönetimi çerçevelerini, metodolojilerini ve yönergelerini uygulayın ve düzenlemelere ve standartlara uygunluğu sağlayın • Kuruluşun kalite ve risk yönetimi uygulamalarını analiz etmek ve konsolide etmek • İş varlıkları sahiplerinin, yöneticilerin ve diğer paydaşların riskleri yönetmek ve azaltmak için riske dayalı kararlar almalarını sağlayın • Siber güvenlik riskine duyarlı bir ortam oluşturun • İlgili paydaşlarla iletişim kurmak, sunmak ve raporlamak • Risk paylaşımı seçenekleri önerin ve yönetin

Anahtar bilgi	• Risk yönetimi standartları, metodolojileri ve çerçeveleri • Risk yönetimi araçları • Risk yönetimi önerileri ve en iyi uygulamalar • Siber tehditler • Bilgisayar sistemleri güvenlik açıkları • Siber güvenlik kontrolleri ve çözümleri • Siber güvenlik riskleri • Siber güvenlik kontrollerinin etkinliğini izleme, test etme ve değerlendirme • Siber güvenlikle ilgili sertifikalar • Siber güvenlikle ilgili teknolojiler	
e-Yetkinlikler (e-CF'den)	E.3. Risk yönetimi E.5. Süreç geliştirme E.7. İş Değişim Yönetimi E.9. IS-Yönetişim	Seviye 4 3. seviye Seviye 4 Seviye 4

2.11 DİJİTAL ADLİ DENETİM MÜDÜRÜ

Profil başlığı	**Dijital Adli Araştırmacı**
Alternatif Başlık(lar)	Dijital Adli BilişimAnalisti Siber Güvenlik ve Adli BilişimUzmanı Adli Bilişim Danışmanı
Özet beyanı	Siber suç soruşturmasının, kötü amaçlı etkinliği kanıtlamak için tüm dijital kanıtları ortaya çıkardığından emin olun.
Misyon	Eserleri gerçek kişilere bağlar, incelenen dijital sistemlerin tezahürleri, girdileri, çıktıları ve süreçleri dahil olmak üzere verileri yakalar, kurtarır, tanımlar ve korur. Niteliksel bir görüşe dayalı olarak dijital kanıtların analizini, yeniden yapılandırılmasını ve yorumlanmasını sağlar. Elde edilen bulguları yorumlamadan tarafsız bir nitel görüş sunar.
Yükümlülük	• Dijital Adli Analiz Sonuçları • Elektronik Kanıt
Ana görevler)	• Dijital adli soruşturma politikası, planları ve prosedürleri geliştirin • Dijital kanıtları tanımlayın, kurtarın, ayıklayın, belgeleyin ve analiz edin • Dijital kanıtları koruyun ve koruyun ve yetkili paydaşların kullanımına açın • Yetkisiz ve yasa dışı eylemlerin kanıtları için ortamları inceleyin • Dijital adli analiz bulgularını ve sonuçlarını sistematik ve deterministik olarak belgelemek, raporlamak ve sunmak • Adli test, analiz ve raporlama tekniklerini seçin ve özelleştirin
Anahtar beceriler)	• Etik ve bağımsız çalışmak; iç veya dış aktörler tarafından etkilenmez ve önyargılı değildir • Bütünlüğünü korurken bilgi toplayın • Siber güvenlik olaylarını tanımlayın, analiz edin ve ilişkilendirin • Dijital kanıtları basit, anlaşılır ve anlaşılması kolay bir şekilde açıklayın ve sunun • Ayrıntılı ve gerekçeli soruşturma raporları geliştirin ve iletin

Anahtar bilgi	• Dijital Adli Bilişimönerileri ve en iyi uygulamalar • Dijital Adli Bilişimstandartları, metodolojileri ve çerçeveleri • Dijital adli analiz prosedürleri • Test prosedürleri • Cezai soruşturma prosedürleri, standartları, metodolojileri ve çerçeveleri • Siber güvenlikle ilgili yasa, yönetmelik ve mevzuatlar • Kötü amaçlı yazılım analiz araçları • Siber tehditler • Bilgisayar sistemleri güvenlik açıkları • Siber güvenlik saldırı prosedürleri • İşletim sistemleri güvenliği • Bilgisayar ağları güvenliği • Siber güvenlikle ilgili sertifikalar	
e-Yetkinlikler (e-CF'den)	A.7. Teknoloji Trend İzleme B.3. Test yapmak B.5. Dokümantasyon Üretimi E.3. Risk yönetimi	3. seviye Seviye 4 3. seviye 3. seviye

2.12 PENETRASYON TEST UZMANI

Profil başlığı	**Penetrasyon test uzmanı**
Alternatif Başlık(lar)	Pentester Etik Hacker Güvenlik Açığı Analisti Siber Güvenlik Test Uzmanı Saldırgan Siber Güvenlik Uzmanı Savunma Siber Güvenlik Uzmanı Kırmızı Takım Uzmanı kırmızı takım arkadaşı
Özet beyanı	Güvenlik kontrollerinin etkinliğini değerlendirin, siber güvenlik açıklarını ortaya çıkarın ve kullanın, tehdit aktörleri tarafından sömürülmeleri durumunda kritikliklerini değerlendirin.
Misyon	Dağıtılan veya planlanan güvenlik önlemlerinin etkinliğini değerlendirmek için sızma testi faaliyetleri ve saldırı senaryoları planlar, tasarlar, uygular ve yürütür. BİT ürünlerinin (örneğin sistemler, donanım, yazılım ve hizmetler) gizliliğini, bütünlüğünü ve kullanılabilirliğini etkileyen teknik ve organizasyonel kontrollerdeki güvenlik açıklarını veya arızaları tanımlar.
Yükümlülük	• Güvenlik Açığı Değerlendirme Sonuçları Raporu • Sızma Testi Raporu
Ana görevler)	• Teknik ve organizasyonel siber güvenlik açıklarını belirleyin, analiz edin ve değerlendirin • Saldırı vektörlerini belirleyin, teknik siber güvenlik açıklarından yararlanıldığını ortaya çıkarın ve gösterin • Test sistemleri ve operasyonların düzenleyici standartlara uygunluğu • Uygun sızma testi tekniklerini seçin ve geliştirin • Sızma testi için test planları ve prosedürleri düzenleyin • Sızma testi sonuç analizi ve raporlaması için prosedürler oluşturun • Sızma testi sonuçlarını belgeleyin ve paydaşlara bildirin • Penetrasyon testi araçlarını ve test programlarını dağıtın

Anahtar beceriler)	• Kodlar, komut dosyaları ve programlar geliştirin • sosyal mühendislik yap • Güvenlik açıklarını tanımlayın ve kullanın • Etik hackleme yapmak • Yaratıcı ve kutunun dışında düşünün • Siber güvenlikle ilgili sorunları belirleyin ve çözün • İlgili paydaşlarla iletişim kurmak, sunmak ve raporlamak • Sızma testi araçlarını etkin bir şekilde kullanın • Teknik analiz ve raporlama yapmak • Zayıflıkları ve etkisiz kontrolleri belirlemek için sistemleri ayrıştırın ve analiz edin • Kodları gözden geçirin, güvenliklerini değerlendirin	
Anahtar bilgi	• Siber güvenlik saldırı prosedürleri • Bilgi teknolojisi (BT) ve operasyonel teknoloji (OT) cihazları • Saldırı ve savunma güvenlik prosedürleri • İşletim sistemleri güvenliği • Bilgisayar ağları güvenliği • Penetrasyon testi prosedürleri • Sızma testi standartları, metodolojileri ve çerçeveleri • Penetrasyon test araçları • Bilgisayar Programlama • Bilgisayar sistemleri güvenlik açıkları • Siber güvenlik önerileri ve en iyi uygulamalar • Siber güvenlikle ilgili sertifikalar	
e-Yetkinlikler (e-CF'den)	B.2. Bileşen Entegrasyonu B.3. Test yapmak B.4. Çözüm Dağıtımı B.5. Dokümantasyon Üretimi	Seviye 4 Seviye 4 Seviye 2 3. seviye
	E.3. Risk yönetimi	Seviye 4

3. İlgili Rol / Görev Tanımları

Çıktı listesi, her bir rol profilinin çıktısı/çıktılarının/çıktılarının/çıktılarının bazı gösterge niteliğinde ve pratik örneklerini sağlar. Listelenen çıktılar, liste kapsamlı olmadığı ve dolayısıyla her bir profilin her yönünü kapsamadığı için örnek olarak sunulmaktadır.

Profil başlığı	teslim edilebilir	Tanım
Baş Bilgi Güvenliği Görevlisi (CISO)	Siber Güvenlik Stratejisi	Siber Güvenlik Stratejisi, bir kuruluşun altyapılarının ve hizmetlerinin güvenliğini ve esnekliğini geliştirmek için tasarlanmış bir eylem planıdır.
Baş Bilgi Güvenliği Görevlisi (CISO)	Siber Güvenlik Politikası	Kuruluşun siber güvenliğini sağlamak için bir politika listeleme kuralları.
Siber Olay Müdahalecisi	Olay Müdahale Planı	Bir olay müdahalesinin her aşamasında (Hazırlık, Tespit ve Analiz, Muhafaza, Eradikasyon ve Kurtarma, Olay Sonrası) atılması gereken adımları detaylandıran bir dizi belgelenmiş prosedür Aktivite).
Siber Olay Müdahalecisi	Siber Olay Raporu	Bir veya daha fazla siber olayla ilgili ayrıntıları sağlayan bir rapor.
Siber Hukuk, Politika ve Uyum Görevlisi	Uyumluluk Kılavuzu	Bir kuruluşun mevzuata uygunluk yükümlülüklerinin kapsamlı bir şekilde anlaşılmasını sağlayan bir kılavuz. Kanunlara, yönetmeliklere ve/veya standartlara uygunluğu sağlamak için dahili politikalar veya prosedürler içerebilir.
Siber Hukuk, Politika ve Uyum Görevlisi	Uyumluluk raporu	Bir kuruluşun uyum duruşunun mevcut durumunu sunan bir rapor.
Siber Tehdit İstihbarat Uzmanı	Siber Tehdit İstihbaratı Kılavuzu (veya El Kitabı)	Siber tehdit istihbaratı toplama ve/veya paylaşma için araçlar ve/veya metodolojiler sunan bir kılavuz.
Siber Tehdit İstihbarat Uzmanı	Siber Tehdit Raporu	Tehditlere, tehdit aktörlerine ve/veya saldırı tekniklerine ilişkin olarak gözlenen başlıca tehditleri, ana eğilimleri tanımlayan bir rapor. Rapor, ilgili etki azaltma önlemlerini de içerebilir.
Siber Güvenlik Mimarı	Siber Güvenlik Mimarisi Şeması	Varlıkları siber saldırılara karşı korumak için kullanılan bir kuruluşun siber güvenlik sistemi mimarisinin görsel bir temsili.
Siber Güvenlik Mimarı	Siber güvenlik Gereksinim Raporu	Bir sistemin siber güvenliğini sağlamak için gereken bir dizi gereksinimi listeleyen bir rapor.
Siber Güvenlik Denetçisi	Siber Güvenlik Denetim Planı	Denetçinin siber güvenlik denetimi yapmak için izleyeceği genel stratejiyi ve prosedürleri sunan bir plan.
Siber Güvenlik Denetçisi	Siber Güvenlik Denetim Raporu	Bir sistemin güvenlik düzeyinin kapsamlı bir şekilde anlaşılmasını sağlayan, siber güvenlikteki güçlü ve zayıf yönlerini değerlendiren bir rapor. Ayrıca, sistemin genel siber güvenliğini iyileştirmek için iyileştirme eylemleri sağlayabilir.

Siber Güvenlik Eğitimcisi	Siber Güvenlik Farkındalık Programı	Siber güvenlikle ilgili konularda farkındalığı artırmak için bir faaliyet programı (örneğin saldırılarla ilgili dersler)
		ve tehditler) kuruluşların ilgili siber güvenlik risklerini önlemelerine ve azaltmalarına yardımcı olur.
Siber Güvenlik Eğitimcisi	Siber Güvenlik Eğitim Materyali	Bireyleri eğitmek veya becerilerini geliştirmek için siber güvenlikle ilgili kavramları, metodolojileri ve araçları açıklayan materyal. Öğretmenler için El Kitapları, öğrenciler için Araç Setleri ve/veya uygulamalı eğitim oturumlarını desteklemek için Sanal Görseller içerebilir.
Siber Güvenlik Uygulayıcı	Siber Güvenlik Çözümleri	Siber güvenlik çözümleri, kuruluşları siber saldırılara karşı korumayı amaçlayan araçlar ve hizmetler içerebilir.
Siber Güvenlik Araştırmacısı	Siber Güvenlikte Yayın	Siber güvenlik bağlamında araştırma bulgularını ve sonuçlarını yayınlayan akademik yayın. Yayının amacı, teknolojiyi ilerletmek ve/veya yeni yenilikçi çözümler geliştirmek olabilir.
Siber Güvenlik Risk Yöneticisi	Siber Güvenlik Risk Değerlendirme Raporu	Bir sistemin siber güvenlik risklerinin tanımlanması, analizi ve değerlendirilmesinin sonuçlarını listeleyen bir rapor. Ayrıca, tanımlanan riskleri kabul edilebilir bir düzeye indirmek veya azaltmak için kontroller içerebilir.
Siber Güvenlik Risk Yöneticisi	Siber Güvenlik Riski İyileştirme Eylem Planı	Siber güvenlik risklerini azaltmayı amaçlayan hafifletme önlemlerinin uygulanmasıyla ilgili faaliyetleri listeleyen bir eylem planı.
Dijital Adli Araştırmacı	Dijital Adli Analiz Sonuçları	Kötü niyetli olayların olası kanıtlarını ortaya çıkaran ve olası tehdit aktörlerini belirleyen dijital verilerin analizinin sonuçları.
Dijital Adli Araştırmacı	Elektronik Kanıt	İşlevi bir yazılım programına veya bir bilgisayar sistemi veya ağı üzerinde depolanan veya bu ağ üzerinden iletilen verilere bağlı olan, herhangi bir cihazın içerdiği veya ürettiği verilerden elde edilen potansiyel kanıt. (örneğin, günlüklerin doğru toplanması)
Penetrasyon Test Uzmanı	Güvenlik Açığı Değerlendirme Sonuçları Raporu	Bir (genellikle otomatik) güvenlik açığı taraması sırasında bir sistemde ortaya çıkarılan güvenlik açıklarının kritikliğini listeleyen ve değerlendiren bir rapor. Rapor ayrıca temel iyileştirme eylemleri önerebilir.
Penetrasyon Test Uzmanı	Sızma Testi Raporu	Bir güvenlik testi sırasında tanımlanan bir sistemin güvenlik açıklarının ayrıntılı ve kapsamlı bir analizini sağlayan bir rapor. Rapor ayrıca önerilen iyileştirme eylemlerini de içerebilir.