CIS Kontrol	CIS Koruması	Varlık Türü	Güvenlik Fonksiyonu	Başlık	Açıklama	IG1	IG2	IG3	v7.1 CIS Koruması	v7.1 CIS Koruma Başlığı	Aynı CSC'de Yeniden Sıralama	Farklı CSC'de Yeniden Sıralama	Yeni	Birleştirilmiş içerik	IG'lerin v7.1'den Genişletilmesi	IG'lerin v7.1'den Düşürülmesi	IG'ler v7.1'den Aynı Kalması
1	1,3	Cihazlar	Tespit et (Detect)	Aktif keşif aracını kullanmak	Kurumsal ağına bağlı varlıkları belirlemek için aktif bir keşif aracı kullanın. Aktif keşif aracını günlük veya daha sık çalışacak şekilde yapılandırın.		x	x	1,1	Aktif keşif aracını kullanmak	x						x
1	1,5	Cihazlar	Tespit et (Detect)	Pasif Varlık Keşif Aracı kullanmak	Kurumsal ağına bağlı varlıkları belirlemek için aktif bir keşif aracı kullanın. Haftada en az bir veya daha sık kurumun varlık envanterini güncellemek için taramaları gözden geçirin ve kullanın.			x	1,2	Pasif Varlık Keşif Aracı kullanmak	x			x			x
1	1,4	Cihazlar	Tanımla (Identify)	Kurumsal Varlık Envanterini Güncellemek için Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) Günlüğünü Kullanmak	Kuruluşun varlık envanterini güncellemek için tüm DHCP sunucularında veya İnternet Protokolü (IP) adres yönetim araçlarında DHCP günlüğünü kullanın. Kuruluşun varlık envanterini haftalık veya daha sık güncellemek için günlükleri inceleyin ve kullanın.		x	x	1,3	Varlık Envanterini Güncellemek için DHCP Günlüğünü Kullanmak	x						x
1	1,1	Cihazlar	Tanımla (Identify)	Ayrıntılı Kurumsal Varlık Envanteri Oluşturmak ve Bakımını Yapmak	Son kullanıcı cihazları (taşınabilir ve mobil dahil), ağ cihazları, bilgi işlem dışı/IoT cihazları ve sunucuları içerecek şekilde, verileri depolama veya işleme potansiyeline sahip tüm kurumsal varlıkların doğru, ayrıntılı ve güncel bir envanterini oluşturun ve bakımını yapın. Envanterin ağ adresini (statikse), donanım adresini, makine adını, kurumsal varlık sahibini, her varlık için departmanı ve varlığın ağa bağlanmak için onaylanıp onaylanmadığını kaydettiğinden emin olun.Mobil son kullanıcı cihazları için, uygun olduğunda MDM türü araçlar bu süreci destekleyebilir. Bu envanter, fiziksel, sanal, uzaktan ve bulut ortamlarındaki altyapıya bağlı öğeleri içerir.Ek olarak, kuruluşun kontrolü altında olmasalar bile kuruluşun ağ altyapısına düzenli olarak bağlanan varlıkları içerir. Tüm kurumsal varlıkların envanterini iki yılda bir veya daha sık gözden geçirin ve güncelleyin.	x	x	x	1,4	Ayrıntılı Varlık Envanterini Koruyun	x			x	x		
1	1,1	Cihazlar	Tanımla (Identify)	Ayrıntılı Kurumsal Varlık Envanteri Oluşturun ve Bakımını Yapın	Son kullanıcı cihazları (taşınabilir ve mobil dahil), ağ cihazları, bilgi işlem dışı/IoT cihazlar ve sunucular dahil olmak üzere, veri depolama veya işleme potansiyeline sahip tüm kurumsal varlıkların doğru, ayrıntılı ve güncel bir envanterini oluşturun ve bakımını yapın.Envanterin ağ adresini (statikse), donanım adresini, makine adını, kurumsal varlık sahibini, her varlık için departmanı ve varlığın ağa bağlanmak için onaylanıp onaylanmadığını kaydettiğinden emin olun.Mobil son kullanıcı cihazları için, uygun olduğunda MDM türü araçlar bu süreci destekleyebilir.Bu envanter, fiziksel, sanal, uzaktan ve bulut ortamlarındaki altyapıya bağlı öğeleri içerir.Ek olarak, kuruluşun kontrolü altında olmasalar bile kuruluşun ağ altyapısına düzenli olarak bağlanan varlıkları içerir.Tüm kurumsal varlıkların envanterini iki yılda bir veya daha sık gözden geçirin ve güncelleyin.	x	x	x	1,5	Varlık Envanteri Bilgilerini Koru	x			x	x		
1	1,2	Cihazlar	Cevapla (Respond)	Yetkisiz Varlıkları Adresleyin	Yetkisiz varlıkları haftalık olarak ele almak için bir sürecin var olduğundan emin olun. Kurum, varlığı ağdan kaldırmayı, varlığın ağa uzaktan bağlanmasını engellemeyi veya varlığı karantinaya almayı seçebilir.	x	x	x	1,6	Yetkisiz Varlıkları Adresleyin	x						x
13	13,9	Cihazlar	Koruma (Protect)	Bağlantı noktasını dağıt -Level Access Control	Bağlantı noktası düzeyinde erişim denetimi dağıtın. Bağlantı noktası düzeyinde erişim denetimi, 802.1x veya sertifikalar gibi benzer ağ erişim denetimi protokollerini kullanır ve kullanıcı ve/veya cihaz kimlik doğrulamasını içerebilir.			x	1,7	Bağlantı Noktası Düzeyinde Erişim Denetimi Dağıtın		x		x		x	
13	13,9	Cihazlar	Koruma (Protect)	Dağıt Port-Level Access Control	Bağlantı noktası düzeyinde erişim denetimi dağıtın Bağlantı noktası düzeyinde erişim denetimi, 802.1x veya sertifikalar gibi benzer ağ erişim denetimi protokollerini kullanır ve kullanıcı ve/veya cihaz kimlik doğrulamasını içerebilir.			x	1,8	Donanım Varlıklarını Doğrulamak için İstemci Sertifikalarını Kullanın		x		x			x
2	2,1	Uygulamalar	Tanımla (Identify)	Bir Yazılım Envanteri Oluşturun ve Bakımını Yapın	Kurumsal varlıklara kurulu tüm lisanslı yazılımların ayrıntılı bir envanterini oluşturun ve bakımını yapın. Yazılım envanteri, her giriş için başlığı, yayıncıyı, ilk kurulum/kullanım tarihini ve iş amacını belgelemelidir; uygun olduğunda, Tekdüzen Kaynak Bulucu (URL), uygulama mağaza(lar), sürüm(ler), dağıtım mekanizması ve kullanımdan kaldırma tarihini ekleyin. Yazılım envanterini yılda iki kez veya daha sık gözden geçirin ve güncelleyin.	x	x	x	2,1	Yetkili Yazılım Envanterini Koruyun	x			x	x		
2	2,2	Uygulamalar	Tanımla (Identify)	Yetkili Yazılımın Şu Anda Desteklendiğinden Emin Olun	Kurumsal varlıklar için yazılım envanterinde yalnızca şu anda desteklenen yazılımın yetkili olarak belirlendiğinden emin olun. Yazılım desteklenmiyorsa ancak kuruluşun misyonunun yerine getirilmesi için gerekliyse, hafifletici kontrolleri ve artık risk kabulünü ayrıntılandıran bir istisna belgeleyin. İstisna belgesi olmayan herhangi bir desteklenmeyen yazılım için yetkisiz olarak atayın. Yazılım desteğini en az ayda bir veya daha sık doğrulamak için yazılım listesini gözden geçirin.	x	x	x	2,2	Yazılımın Satıcı Tarafından Desteklendiğinden Emin Olun	x						x
2	2,4	Uygulamalar	Tespit et (Detect)	Otomatik Yazılım Envanteri Araçlarını Kullanın	Kurulu yazılımların keşfedilmesini ve belgelenmesini otomatikleştirmek için mümkün olduğunda kuruluş genelinde yazılım envanter araçlarını kullanın.		x	x	2,3	Yazılım Envanteri Araçlarını Kullanın	x						x
2	2,1	Uygulamalar	Tanımla (Identify)	Bir Yazılım Envanteri Oluşturun ve Bakımını Yapın	Kurumsal varlıklara kurulu tüm lisanslı yazılımların ayrıntılı bir envanterini oluşturun ve bakımını yapın. Yazılım envanteri, her giriş için başlığı, yayıncıyı, ilk kurulum/kullanım tarihini ve iş amacını belgelemelidir; uygun olduğunda, URL, app storelar, sürüm(ler), dağıtım mekanizması ve kullanımdan kaldırma tarihini ekleyin. Yazılım envanterini yılda iki kez veya daha sık gözden geçirin ve güncelleyin.	x	x	x	2,4	Yazılım Envanteri Bilgilerini Takip Edin	x			x	x		
2	2,3	Uygulamalar	Cevapla (Respond)	Yetkisiz Yazılımı Adresleyin	Yetkisiz yazılımın kurumsal varlıklarda kullanımdan kaldırıldığından veya belgelenmiş bir istisna aldığından emin olun. Aylık veya daha sık gözden geçirin.	x	x	x	2,6	Onaylanmamış Yazılımın Adresi	x						x
2	2,5	Uygulamalar	Koruma (Protect)	İzin Verilenler Yetkili Yazılım Listesi	Yalnızca yetkili yazılımın çalıştırılabilmesini veya erişilebilmesini sağlamak için izin verilenler listesine uygulama gibi teknik kontrolleri kullanın. İki yılda bir veya daha sık olarak yeniden değerlendirin.		x	x	2,7	Uygulama Beyaz Listesini Kullanın	x				x		
2	2,6	Uygulamalar	Koruma (Protect)	İzin Verilenler Yetkili Kitaplıklar(libraries) Listesi	Yalnızca belirli .dll, .ocx, .so vb. dosyalar gibi yetkili yazılım kitaplıklarının bir sistem işlemine yüklenmesine izin verildiğinden emin olmak için teknik kontrolleri kullanın. Yetkisiz kitaplıkların bir sistem işlemine yüklenmesini engelleyin. İki yılda bir veya daha sık olarak yeniden değerlendirin.		x	x	2,8	Kitaplıkların Uygulama Beyaz Listesini Uygulayın	x				x		
2	2,7	Uygulamalar	Koruma (Protect)	İzin Verilen Yetkilendirilmiş Komut Dosyaları Listesi(scripts)	Yalnızca belirli .ps1, .py vb. dosyalar gibi yetkili komut dosyalarının yürütülmesine izin verildiğinden emin olmak için dijital imzalar ve sürüm denetimi gibi teknik denetimleri kullanın. Yetkisiz komut dosyalarının yürütülmesini engelleyin. İki yılda bir veya daha sık olarak yeniden değerlendirin.			x	2,9	Komut Dosyalarının Uygulama Beyaz Listesini Uygulayın	x			x			x
3	3,12	Ağ	Koruma (Protect)	Hassasiyete Dayalı Segment Veri İşleme ve Depolama	Verilerin hassasiyetine göre veri işleme ve depolamayı bölümlere ayırın. Daha düşük hassasiyetli verilere yönelik kurumsal varlıklardaki hassas verileri işlemeyin.		x	x	2,10	Yüksek Riskli Uygulamaları Fiziksel veya Mantıksal Olarak Ayırın		x		x	x		
7	7,5	Uygulamalar	Tanımla (Identify)	Dahili Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin	Dahili kurumsal varlıkların otomatik güvenlik açığı taramalarını üç ayda bir veya daha sık aralıklarla gerçekleştirin. SCAP uyumlu bir güvenlik açığı tarama aracı kullanarak hem kimliği doğrulanmış hem de kimliği doğrulanmamış taramalar gerçekleştirin.		x	x	3,1	Otomatik Güvenlik Açığı Tarama Araçlarını Çalıştırın	x			x			x
7	7,6	Uygulamalar	Tanımla (Identify)	Dışarıdan Tespit Edilen Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin	SCAP uyumlu bir güvenlik açığı tarama aracı kullanarak harici olarak açığa çıkan kurumsal varlıkların otomatik güvenlik açığı taramalarını gerçekleştirin. Taramaları aylık veya daha sık aralıklarla gerçekleştirin.		x	x	3,1	Otomatik Güvenlik Açığı Tarama Araçlarını Çalıştırın	x			x			x
7	7,5	Uygulamalar	Tanımla (Identify)	Dahili Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin	Dahili kurumsal varlıkların otomatik güvenlik açığı taramalarını üç ayda bir veya daha sık aralıklarla gerçekleştirin. SCAP uyumlu bir güvenlik açığı tarama aracı kullanarak hem kimliği doğrulanmış hem de kimliği doğrulanmamış taramalar gerçekleştirin.		x	x	3,2	Kimliği Doğrulanmış Güvenlik Açığı Taraması Gerçekleştirin	x			x			x
5	5,5	Kullanıcılar	Tanımla (Identify)	Hizmet Hesapları Envanteri Oluşturun ve Bakımını Yapın	Hizmet hesaplarının bir envanterini oluşturun ve bakımını yapın. Envanter, en azından departman sahibini, gözden geçirme tarihini ve amacını içermelidir. Tüm etkin hesapların yetkilendirildiğini doğrulamak için, en az üç ayda bir veya daha sık aralıklarla yinelenen bir programda hizmet hesabı incelemeleri gerçekleştirin.		x	x	3,3	Özel Değerlendirme Hesaplarını Koruyun		x		x			x
7	7,3	Uygulamalar	Koruma (Protect)	Otomatik İşletim Sistemi Yama Yönetimini Gerçekleştirin	Aylık veya daha sık aralıklarla otomatik yama yönetimi aracılığıyla kurumsal varlıklarda işletim sistemi güncellemeleri gerçekleştirin.	x	x	x	3,4	Otomatik İşletim Sistemi Yama Yönetim Araçlarını Dağıtın	x						x
7	7,4	Uygulamalar	Koruma (Protect)	Otomatik Uygulama Yama Yönetimini Gerçekleştirin	Aylık veya daha sık aralıklarla otomatik yama yönetimi aracılığıyla kurumsal varlıklarda uygulama güncellemeleri gerçekleştirin.	x	x	x	3,5	Otomatik Yazılım Yama Yönetim Araçlarını Dağıtın	x			x			x
7	7,2	Uygulamalar	Cevapla (Respond)	Bir İyileştirme Süreci Oluşturun ve bakımını yapın	Aylık veya daha sık gözden geçirmelerle bir iyileştirme sürecinde belgelenen riske dayalı bir iyileştirme stratejisi oluşturun ve bakımını yapın.	x	x	x	3,6	Arka Arkaya Güvenlik Açığı Taramalarını Karşılaştırın	x			x			x
7	7,2	Uygulamalar	Cevapla (Respond)	Bir İyileştirme Süreci Oluşturun ve bakımını yapın	Aylık veya daha sık gözden geçirmelerle bir iyileştirme sürecinde belgelenen riske dayalı bir iyileştirme stratejisi oluşturun ve bakımını yapın.	x	x	x	3,7	Risk Derecelendirme Sürecinden Yararlanın	x			x			x
16	16,6	Uygulamalar	Koruma (Protect)	Uygulama Güvenlik Açıkları için Önem Derecelendirme Sistemi ve Süreci Oluşturun ve Sürdürün	Keşfedilen güvenlik açıklarının düzeltildiği sıraya öncelik verilmesini kolaylaştıran uygulama güvenlik açıkları için bir önem derecesi derecelendirme sistemi ve süreci oluşturun ve sürdürün. Bu süreç, kod veya uygulamaları serbest bırakmak için minimum güvenlik kabul edilebilirliği düzeyini ayarlamayı içerir. Önem dereceleri, risk yönetimini geliştiren ve en ciddi hataların ilk önce düzeltilmesini sağlamaya yardımcı olan güvenlik açıklarını tetiklemek için sistematik bir yol sunar. Sistemi ve süreci yıllık olarak gözden geçirin ve güncelleyin.		x	x	3,7	Risk Derecelendirme Sürecinden Yararlanın		x					x
18	18,3	Ağ	Koruma (Protect)	Penetrasyon Testi Bulgularını Düzeltin	Kuruluşun iyileştirme kapsamı ve önceliklendirme politikasına dayalı olarak sızma testi bulgularını düzeltin.		x	x	3,7	Risk Derecelendirme Sürecinden Yararlanın		x					x
5	5,1	Kullanıcılar	Tanımla (Identify)	Accounts(hesap) Envanteri Oluşturun ve Bakımını Yapın	Kuruluşta yönetilen tüm hesapların bir envanterini oluşturun ve bakımını yapın. Envanter hem kullanıcı hem de yönetici hesaplarını içermelidir. Envanter en azından kişinin adını, kullanıcı adını, başlangıç/bitiş tarihlerini ve departmanını içermelidir. Tüm aktif hesapların, en az üç ayda bir veya daha sık aralıklarla yinelenen bir programa göre yetkilendirildiğini doğrulayın.	x	x	x	4,1	İdari Hesapların Envanterini Koru	x			x	x		
4	4,7	Kullanıcılar	Koruma (Protect)	Kurumsal Varlıklar ve Yazılımlarda Varsayılan Hesapları Yönetin	Kök, yönetici ve diğer önceden yapılandırılmış satıcı hesapları gibi kurumsal varlıklar ve yazılımlardaki varsayılan hesapları yönetin. Örnek uygulamalar şunları içerebilir: varsayılan hesapları devre dışı bırakmak veya kullanılamaz hale getirmek.	x	x	x	4,2	Varsayılan Parolaları Değiştir		x					x
5	5,4	Kullanıcılar	Koruma (Protect)	Yönetici Ayrıcalıklarını Özel Yönetici Hesaplarıyla Kısıtlayın	Yönetici ayrıcalıklarını, kurumsal varlıklarda özel olarak ayrılmış yönetici hesaplarıyla sınırlayın. Kullanıcının birincil, ayrıcalıklı olmayan hesabından internette gezinme, e-posta ve üretkenlik paketi kullanımı gibi genel bilgi işlem etkinliklerini gerçekleştirin.	x	x	x	4,3	Özel İdari Hesapların Kullanılmasını Sağlayın	x						x
5	5,2	Kullanıcılar	Koruma (Protect)	Benzersiz Parolalar Kullanın(Unique)	Tüm kurumsal varlıklar için benzersiz parolalar kullanın. En iyi uygulama uygulaması, MFA kullanan hesaplar için en az 8 karakterlik bir şifre ve MFA kullanmayan hesaplar için 14 karakterlik bir şifre içerir.	x	x	x	4,4	Benzersiz Parolalar Kullanın	x				x		
6	6,5	Kullanıcılar	Koruma (Protect)	Yönetici Erişimi için MFA gerektir	Desteklendiğinde, yerinde veya bir üçüncü taraf sağlayıcı aracılığıyla yönetilen tüm kurumsal varlıklarda tüm yönetim erişim hesapları için MFA gerektir.	x	x	x	4,5	Tüm Yönetim Erişimi için Çok Faktörlü Kimlik Doğrulamayı Kullanın	x						x
12	12,8	Cihazlar	Koruma (Protect)	Tüm İdari İşler için Özel Bilgi İşlem Kaynakları Oluşturun ve Bakımını Yapın	Tüm idari görevler veya idari erişim gerektiren görevler için fiziksel veya mantıksal olarak ayrılmış özel bilgi işlem kaynakları oluşturun ve sürdürün. Bilgi işlem kaynakları, işletmenin birincil ağından bölümlere ayrılmalı ve internet erişimine izin verilmemelidir.			x	4,6	Tüm Yönetim Görevleri İçin Özel İş İstasyonları Kullanın	x			x			x
2	2,7	Uygulamalar	Koruma (Protect)	İzin Verilen Yetkilendirilmiş Komut Dosyaları(i Scripts) Listesi	Yalnızca belirli .ps1, .py vb. dosyaları gibi yetkili komut dosyalarının yürütülmesine izin verildiğinden emin olmak için dijital imzalar ve sürüm denetimi gibi teknik denetimleri kullanın. Yetkisiz komut dosyalarının yürütülmesini engelleyin. İki yılda bir veya daha sık olarak yeniden değerlendirin.			x	4,7	Komut Dosyası Araçlarına Erişimi Sınırlayın		x		x		x	
8	8,5	Ağ	Tespit et (Detect)	Ayrıntılı Denetim Günlüklerini(Logs) Toplayın	Hassas veriler içeren kurumsal varlıklar için ayrıntılı denetim günlüğünü yapılandırın. Adli soruşturmaya yardımcı olabilecek olay kaynağı, tarih, kullanıcı adı, zaman damgası, kaynak adresleri, hedef adresleri ve diğer yararlı öğeleri dahil edin.		x	x	4,8	İdari Grup Üyeliğindeki Değişiklikleri Günlüğe Kaydet ve Uyarı mesajı gönder		x		x	x		
8	8,5	Ağ	Tespit et (Detect)	Ayrıntılı Denetim Günlüklerini Toplayın	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		x	x	4,9	Başarısız İdari Hesap Girişinde Oturum Açın ve Uyarı Mesajı Gönderin		x		x	x		
4	4,1	Uygulamalar	Koruma (Protect)	Güvenli Bir Yapılandırma Süreci Oluşturun ve Bakımını yapın	Kurumsal varlıklar (taşınabilir ve mobil dahil son kullanıcı cihazları; bilgi işlem dışı/IoT cihazları ve sunucular) ve yazılımlar (işletim sistemleri ve uygulamaları) için güvenli bir yapılandırma süreci oluşturun ve sürdürün. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	5,1	Güvenli Yapılandırmalar Oluşturun	x			x			x

4	4,1	Uygulamalar	Koruma (Protect)	Güvenli Bir Yapılandırma Süreci Oluşturun ve Sürdürün	Kurumsal varlıklar (taşınabilir ve mobil dahil son kullanıcı cihazları; bilgi işlem dışı/IoT cihazları ve sunucular) ve yazılımlar (işletim sistemleri ve uygulamaları) için güvenli bir yapılandırma süreci oluşturun ve sürdürün. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	5,4	**Sistem Yapılandırma Yönetim Aracını Dağıtın**				x	x		
8	8,4	Ağ	Koruma (Protect)	Zaman Senkronizasyonunu Standartlaştırın	Zaman senkronizasyonunu standartlaştırın. Destekleniyorsa, kurumsal varlıklar genelinde en az iki senkronize zaman kaynağı yapılandırın		x	x	6,1	**Üç Senkronize Zaman Kaynağını Kullanın**	x						x
8	8,2	Ağ	Tespit et (Detect)	Denetim Günlüklerini Toplayın(logs)	Denetim günlüklerini toplayın. Kuruluşun denetim günlüğü yönetim süreci uyarınca günlük kaydının kurumsal varlıklar genelinde etkinleştirildiğinden emin olun.	x	x	x	6,2	**Denetim Günlüğünü Etkinleştir**	x			x			x
8	8,5	Ağ	Tespit et (Detect)	Ayrıntılı Denetim Günlüklerini Toplayın	Hassas veriler içeren kurumsal varlıklar için ayrıntılı denetim günlüğünü yapılandırın. Adli soruşturmaya yardımcı olabilecek olay kaynağı, tarih, kullanıcı adı, zaman damgası, kaynak adresleri, hedef adresleri ve diğer yararlı öğeleri dahil edin.		x	x	6,3	**Ayrıntılı Günlüğü Etkinleştir**	x						x
8	8,3	Ağ	Koruma (Protect)	Yeterli Denetim Günlüğü Depolamasını Sağlayın	Günlüğe kaydetme hedeflerinin, kuruluşun denetim günlüğü yönetimi sürecine uymak için yeterli depolamayı sürdürdüğünden emin olun.	x	x	x	6,4	**Günlükler için Yeterli Depolamayı Sağlayın**	x						x
8	8,9	Ağ	Tespit et (Detect)	Denetim Günlüklerini Merkezileştirin	Kurumsal varlıklar genelinde denetim günlüğü toplama ve saklamayı mümkün olduğu ölçüde merkezileştirin.		x	x	6,5	**Merkezi Günlük Yönetimi**	x						x
13	13,1	Ağ	Tespit et (Detect)	Güvenlik Olayı Uyarısını Merkezileştirin	Günlük korelasyonu ve analizi için güvenlik olayı uyarılarını kurumsal varlıklar genelinde merkezileştirin. En iyi uygulama uygulaması, satıcı tanımlı olay bağıntı uyarılarını içeren bir SIEM kullanımını gerektirir. Güvenlikle ilgili korelasyon uyarılarıyla yapılandırılmış bir günlük analizi platformu da bu Korumayı karşılar.		x	x	6,6	**SIEM veya Log Analitik Araçlarını Dağıtın**		x					x
8	8,11	Ağ	Tespit et (Detect)	Denetim Günlüğü İncelemelerini Yürütün	Olası bir tehdidi gösterebilecek anormallikleri veya anormal olayları tespit etmek için denetim günlüklerini gözden geçirin. İncelemeleri haftalık veya daha sık aralıklarla gerçekleştirin.		x	x	6,7	**Günlükleri Düzenli Olarak Gözden Geçirin**	x						x
13	13,11	Ağ	Tespit et (Detect)	Güvenlik Olayı Uyarı Eşiklerini Ayarlayın	Güvenlik olayı uyarı eşiklerini aylık olarak veya daha sık ayarlayın.			x	6,8	**SIEM'i Düzenli Olarak Ayarlayın**		x					x
9	9,1	Uygulamalar	Koruma (Protect)	Yalnızca Tam Olarak Desteklenen Tarayıcıların ve E-posta İstemcilerinin Kullanıldığından Emin Olun	Yalnızca satıcı tarafından sağlanan tarayıcıların ve e-posta istemcilerinin en son sürümünü kullanarak kuruluşta yalnızca tam olarak desteklenen tarayıcıların ve e-posta istemcilerinin çalışmasına izin verildiğinden emin olun.	x	x	x	7,1	**Yalnızca Tam Olarak Desteklenen Tarayıcıların ve E-posta İstemcilerinin Kullanıldığından Emin Olun**	x						x
9	9,4	Uygulamalar	Koruma (Protect)	Gereksiz veya Yetkisiz Tarayıcı ve E-posta İstemcisi Uzantılarını Kısıtlayın	Yetkisiz veya gereksiz tarayıcı veya e-posta istemcisi eklentilerini, uzantılarını ve eklenti uygulamalarını kaldırarak veya devre dışı bırakarak kısıtlayın.		x	x	7,2	**Gereksiz veya Yetkisiz Tarayıcı veya E-posta İstemcisi Eklentilerini Devre Dışı Bırakın**	x						x
2	2,7	Uygulamalar	Koruma (Protect)	İzin Verilen Yetkilendirilmiş Komut Dosyaları Listesi	Yalnızca belirli .ps1, .py vb. dosyaları gibi yetkili komut dosyalarının yürütülmesine izin verildiğinden emin olmak için dijital imzalar ve sürüm denetimi gibi teknik denetimleri kullanın. Yetkisiz komut dosyalarının yürütülmesini engelleyin. İki yılda bir veya daha sık aralıklarla yeniden değerlendirin.			x	7,3	**Web Tarayıcılarında ve E-posta İstemcilerinde Komut Dosyası Dillerinin Kullanımını Sınırlayın**		x		x		x	
9	9,3	Ağ	Koruma (Protect)	Ağ Tabanlı URL Filtrelerini Koruyun ve Bakımını Yapın	Bir kurumsal varlığın potansiyel olarak kötü amaçlı veya onaylanmamış web sitelerine bağlanmasını sınırlamak için ağ tabanlı URL filtrelerini zorunlu kılın ve güncelleyin. Örnek uygulamalar, kategori tabanlı filtrelemeyi, itibar tabanlı filtrelemeyi veya engelleme listelerinin kullanımını içerir. Tüm kurumsal varlıklar için filtreler uygulayın.		x	x	7,4	**Ağ Tabanlı URL Filtrelerini Koruyun ve Uygulayın**	x			x			x
9	9,3	Ağ	Koruma (Protect)	Ağ Tabanlı URL Filtrelerini Koruyun ve bakımını yapın	Bir kurumsal varlığın potansiyel olarak kötü amaçlı veya onaylanmamış web sitelerine bağlanmasını sınırlamak için ağ tabanlı URL filtrelerini zorunlu kılın ve güncelleyin. Örnek uygulamalar, kategori tabanlı filtrelemeyi, itibar tabanlı filtrelemeyi veya engelleme listelerinin kullanımını içerir. Tüm kurumsal varlıklar için filtreler uygulayın.		x	x	7,5	**URL Sınıflandırma Hizmetine abone olun**	x			x			x
8	8,7	Ağ	Tespit et (Detect)	URL İsteği Denetim Günlüklerini Toplayın	Uygun ve desteklenen yerlerde, kurumsal varlıklarda URL istek denetim günlüklerini toplayın.		x	x	7,6	**Tüm URL İsteklerini Günlüğe Kaydet**		x					x
9	9,2	Ağ	Koruma (Protect)	DNS Filtreleme Hizmetlerini Kullanın	Bilinen kötü amaçlı etki alanlarına(domains) erişimi engellemek için tüm kurumsal varlıklarda DNS filtreleme hizmetlerini kullanın.	x	x	x	7,7	**DNS Filtreleme Hizmetlerinin Kullanımı**	x			x			x
9	9,5	Ağ	Koruma (Protect)	DMARC'yi uygulayın	Geçerli alanlardan gelen sahte veya değiştirilmiş e-postaların olasılığını azaltmak için Gönderici Politikası Çerçevesi (SPF) ve Etki Alanı Anahtarları Tanımlanmış Posta (DKIM) standartlarını uygulamaya başlayarak DMARC politikasını ve doğrulamasını uygulayın.		x	x	7,8	**DMARC'yi uygulayın ve Alıcı Tarafı Doğrulamayı Etkinleştirin**	x						x
9	9,6	Ağ	Koruma (Protect)	Gereksiz Dosya Türlerini Engelle	Kuruluşun e-posta ağ geçidine girmeye çalışan gereksiz dosya türlerini engelleyin.		x	x	7,9	**Gereksiz Dosya Türlerini Engelle**	x						x
9	9,7	Ağ	Koruma (Protect)	E-posta Sunucusu Kötü Amaçlı Yazılımdan Koruma Korumalarını Dağıtın ve Bakımını Yapın	Ek tarama ve/veya korumalı alan oluşturma gibi e-posta sunucusu kötü amaçlı yazılıma karşı korumaları dağıtın ve bakımını yapın			x	7,10	**Korumalı Alan Tüm E-posta Ekleri**	x			x			x
10	10,6	Cihazlar	Koruma (Protect)	Kötü Amaçlı Yazılımdan Koruma Yazılımını Merkezi Olarak Yönetin	Kötü amaçlı yazılımdan koruma yazılımını merkezi olarak yönetin.		x	x	8,1	**Merkezi Olarak Yönetilen Kötü Amaçlı Yazılımdan Koruma Yazılımını Kullanın**	x						x
10	10,2	Cihazlar	Koruma (Protect)	Otomatik Kötü Amaçlı Yazılımdan Koruma İmza (signature) Güncellemelerini Yapılandırın	Tüm kurumsal varlıklardaki kötü amaçlı yazılımdan koruma imza dosyaları için otomatik güncellemeleri yapılandırın.	x	x	x	8,2	**Kötü Amaçlı Yazılımdan Koruma Yazılımının ve İmzaların Güncellendiğinden Emin Olun**	x						x
10	10,5	Cihazlar	Koruma (Protect)	Sömürü(exploitation) Önleme Özelliklerini Etkinleştir	Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) veya Apple® System Integrity Protection (SIP) ve Gatekeeper™ gibi, kurumsal varlıklarda ve yazılımlarda, mümkün olduğunda, istismar(explotation) önleme özelliklerini etkinleştirin.		x	x	8,3	**İşletim Sistemi İstismarı Önleme Özelliklerini Etkinleştir/ İstismarı Önleme Teknolojilerini Dağıt**	x						x
10	10,4	Cihazlar	Tespit et (Detect)	Çıkarılabilir Ortamın Otomatik Kötü Amaçlı Yazılımdan Koruma Taramasını Yapılandırın	Çıkarılabilir medyayı otomatik olarak taramak için kötü amaçlı yazılımdan koruma yazılımını yapılandırın.		x	x	8,4	**Çıkarılabilir Medyanın Kötü Amaçlı Yazılımdan Koruma Taramasını Yapılandırın**	x					x	
10	10,3	Cihazlar	Koruma (Protect)	Çıkarılabilir Medya için Otomatik Çalıştırmayı ve Otomatik Oynatmayı Devre Dışı Bırakın	Çıkarılabilir medya için otomatik çalıştırma ve otomatik çalıştırma otomatik çalıştırma işlevini devre dışı bırakın.	x	x	x	8,5	**Cihazları İçeriği Otomatik Çalıştırmayacak Şekilde Yapılandırma**	x						x
8	8,2	Ağ	Tespit et (Detect)	Denetim Günlüklerini Toplayın	Denetim günlüklerini toplayın. Kuruluşun denetim günlüğü yönetim süreci uyarınca günlük kaydının kurumsal varlıklar genelinde etkinleştirildiğinden emin olun.	x	x	x	8,6	**Kötü Amaçlı Yazılımdan Koruma Günlüğünü Merkezileştirin**		x		x	x		
8	8,6	Ağ	Tespit et (Detect)	DNS Sorgu Denetim Günlüklerini Toplayın	Uygun ve desteklenen yerlerde, kurumsal varlıklarda DNS sorgusu denetim günlüklerini toplayın.		x	x	8,7	**DNS Sorgu Günlüğünü Etkinleştir**		x					x
8	8,8	Cihazlar	Tespit et (Detect)	Komut Satırı Denetim Günlüklerini Toplayın	Komut satırı denetim günlüklerini toplayın. Örnek uygulamalar arasında PowerShell®, BASH™ ve uzak yönetim terminallerinden denetim günlüklerinin toplanması yer alır.		x	x	8,8	**Komut Satırı Denetim Günlüğünü Etkinleştir**		x					x
1	1,1	Cihazlar	Tanımla (Identify)	Ayrıntılı Kurumsal Varlık Envanteri Oluşturun ve Bakımını Yapın	Son kullanıcı cihazları (taşınabilir ve mobil dahil), ağ cihazları, bilgi işlem dışı/IoT dahil olmak üzere, veri depolama veya işleme potansiyeline sahip tüm kurumsal varlıkların doğru, ayrıntılı ve güncel bir envanterini oluşturun ve sürdürün. cihazlar ve sunucular. Envanterin ağ adresini (statikse), donanım adresini, makine adını, veri varlığı sahibini, her varlık için departmanını ve varlığın ağa bağlanmak için onaylanıp onaylanmadığını kaydettiğinden emin olun. Mobil son kullanıcı cihazları için, uygun olduğunda MDM türü araçlar bu süreci destekleyebilir. Bu envanter, fiziksel, sanal, uzaktan ve bulut ortamlarındaki altyapıya bağlı öğeleri içerir. Ek olarak, kuruluşun kontrolü altında olmasalar bile kuruluşun ağ altyapısına düzenli olarak bağlanan varlıkları içerir. Tüm kurumsal varlıkların envanterini iki yılda bir veya daha sık gözden geçirin ve güncelleyin.	x	x	x	9,1	**Aktif Bağlantı Noktalarını, Hizmetleri ve Protokolleri Varlık Envanteri ile İlişkilendirin**		x		x	x		
4	4,4	Cihazlar	Koruma (Protect)	Sunucularda Güvenlik Duvarı Uygulayın ve Yönetin	Desteklendiği yerlerde sunucularda bir güvenlik duvarı uygulayın ve yönetin. Örnek uygulamalar arasında sanal bir güvenlik duvarı, işletim sistemi güvenlik duvarı veya bir üçüncü taraf güvenlik duvarı aracısı bulunur.	x	x	x	9,2	**Yalnızca Onaylanmış Bağlantı Noktalarının(port), Protokollerin ve Servislerin Çalıştığından Emin Olun**		x		x	x		
4	4,5	Cihazlar	Koruma (Protect)	Son Kullanıcı Cihazlarında Güvenlik Duvarı Uygulama ve Yönetme	Son kullanıcı cihazlarında, açıkça izin verilen hizmetler ve bağlantı noktaları dışındaki tüm trafiği bırakan bir varsayılan reddet kuralıyla, ana bilgisayar tabanlı bir güvenlik duvarı veya bağlantı noktası filtreleme aracı uygulayın ve yönetin.	x	x	x	9,2	**Yalnızca Onaylanmış Bağlantı Noktalarının(port), Protokollerin ve Servislerin Çalıştığından Emin Olun**		x		x	x		x
4	4,8	Cihazlar	Koruma (Protect)	Kurumsal Varlıklar ve Yazılımlarda Gereksiz Hizmetleri Kaldırın veya Devre Dışı Bırakın	Kullanılmayan dosya paylaşım hizmeti, web uygulama modülü veya hizmet işlevi gibi kurumsal varlıklar ve yazılımlardaki gereksiz hizmetleri kaldırın veya devre dışı bırakın.		x	x	9,2	**Yalnızca Onaylanmış Bağlantı Noktalarının(port), Protokollerin ve Servislerin Çalıştığından Emin Olun**		x		x			x
7	7,5	Uygulamalar	Tanımla (Identify)	Dahili Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin	Dahili kurumsal varlıkların otomatik güvenlik açığı taramalarını üç ayda bir veya daha sık aralıklarla gerçekleştirin. SCAP uyumlu bir güvenlik açığı tarama aracı kullanarak hem kimliği doğrulanmış hem de kimliği doğrulanmamış taramalar gerçekleştirin.		x	x	9,3	**Düzenli Otomatik Bağlantı Noktası Taramaları Gerçekleştirin**		x		x			x
7	7,6	Uygulamalar	Tanımla (Identify)	Dışarıdan Tespit Edilen Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin	SCAP uyumlu bir güvenlik açığı tarama aracı kullanarak harici olarak açığa çıkan kurumsal varlıkların otomatik güvenlik açığı taramalarını gerçekleştirin. Taramaları aylık veya daha sık aralıklarla gerçekleştirin.		x	x	9,3	**Düzenli Otomatik Port Taramaları Gerçekleştirin**		x		x			x
4	4,4	Cihazlar	Koruma (Protect)	Sunucularda Güvenlik Duvarı Uygulayın ve Yönetin	Desteklendiği yerlerde sunucularda bir güvenlik duvarı uygulayın ve yönetin. Örnek uygulamalar arasında sanal bir güvenlik duvarı, işletim sistemi güvenlik duvarı veya bir üçüncü taraf güvenlik duvarı aracısı bulunur.	x	x	x	9,4	**Ana Bilgisayar Tabanlı Güvenlik Duvarları veya Port Filtreleme Uygulayın**		x		x			x
4	4,5	Cihazlar	Koruma (Protect)	Son Kullanıcı Cihazlarında Güvenlik Duvarı Uygulama ve Yönetme	Son kullanıcı cihazlarında, açıkça izin verilen hizmetler ve bağlantı noktaları dışındaki tüm trafiği bırakan bir varsayılan reddet kuralıyla, ana bilgisayar tabanlı bir güvenlik duvarı veya bağlantı noktası filtreleme aracı uygulayın ve yönetin.	x	x	x	9,4	**Ana Bilgisayar Tabanlı Güvenlik Duvarları veya Port Filtreleme Uygulayın**		x		x			x
13	13,10	Ağ	Koruma (Protect)	Uygulama Katmanı Filtreleme Gerçekleştirin	Aktarılan hassas verileri şifreleyin. Örnek uygulamalar şunları içerebilir: Aktarım(Transport) Katmanı Güvenliği (TLS) ve Açık Güvenli Kabuk (OpenSSH).			x	9,5	**Uygulama Güvenlik Duvarlarını Uygulayın**		x		x	x		
11	11,2	Veri	Kurtarma (Recover)	Otomatik Yedeklemeler Gerçekleştirin	Kapsam dahilindeki kurumsal varlıkların otomatik yedeklemelerini gerçekleştirin. Verilerin hassasiyetine bağlı olarak yedeklemeleri haftalık olarak veya daha sık çalıştırın.	x	x	x	10,1	**Düzenli Otomatik Yedeklemeler Sağlayın**	x			x			x
11	11,2	Veri	Kurtarma (Recover)	Otomatik Yedeklemeler Gerçekleştirin	Kapsam dahilindeki kurumsal varlıkların otomatik yedeklemelerini gerçekleştirin. Verilerin hassasiyetine bağlı olarak yedeklemeleri haftalık olarak veya daha sık çalıştırın.	x	x	x	10,2	**Komple Sistem Yedeklemeleri Gerçekleştirin**	x			x			x
11	11,5	Veri	Kurtarma (Recover)	Veri Kurtarmayı Test Et	Kapsam dahilindeki kurumsal varlıkların bir örneklemesi için yedek kurtarmayı üç ayda bir veya daha sık test edin.		x	x	10,3	**Yedekleme Ortamındaki Test Verileri**	x						x
11	11,3	Veri	Koruma (Protect)	Kurtarma Verilerini Koruyun	Kurtarma verilerini orijinal verilere eşdeğer kontrollerle koruyun. Gereksinimlere göre referans şifreleme veya veri ayrımı.	x	x	x	10,4	**Yedeklemeleri Koruyun**	x						x
11	11,4	Veri	Kurtarma (Recover)	Kurtarma Verilerinin (recovery data) İzole Edilmiş Bir Eşgörünümünü Oluşturun ve Bakımını Yapın	Kurtarma verilerinin yalıtılmış bir örneğini oluşturun ve sürdürün. Örnek uygulamalar arasında çevrimdışı, bulut veya site dışı sistemler veya hizmetler aracılığıyla sürüm kontrol eden yedekleme hedefleri bulunur. Kapsam dahilindeki kurumsal varlıkların bir örneklemesi için yedek kurtarmayı üç ayda bir veya daha sık olarak test edin.	x	x	x	10,5	**Tüm Yedeklemelerin En Az Bir Çevrimdışı Yedekleme Hedefine Sahip Olduğundan Emin Olun**	x						x
4	4,2	Ağ	Koruma (Protect)	Ağ Altyapısı için Güvenli Bir Yapılandırma Süreci Oluşturun ve Sürdürün	Ağ cihazları için güvenli bir yapılandırma süreci oluşturun ve sürdürün. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	11,1	**Ağ Cihazları için Standart Güvenlik Yapılandırmalarını Koruyun**		x		x	x		
4	4,4	Cihazlar	Koruma (Protect)	Sunucularda Güvenlik Duvarı Uygulayın ve Yönetin	Desteklendiği yerlerde sunucularda bir güvenlik duvarı uygulayın ve yönetin. Örnek uygulamalar arasında sanal bir güvenlik duvarı, işletim sistemi güvenlik duvarı veya bir üçüncü taraf güvenlik duvarı aracısı bulunur.	x	x	x	11,2	**Belge Trafiği Yapılandırma Kuralları**		x		x	x		
4	4,5	Cihazlar	Koruma (Protect)	Son Kullanıcı Cihazlarında Güvenlik Duvarı Uygulama ve Yönetme	Son kullanıcı cihazlarında ana bilgisayar tabanlı bir güvenlik duvarı veya bağlantı noktası filtreleme aracı uygulayın ve yönetin. Açıkça izin verilen hizmetler ve bağlantı noktaları dışındaki tüm trafiği bırakan bir varsayılan reddet(deny) kuralıyla, son kullanıcı cihazlarında ana bilgisayar tabanlı bir güvenlik duvarı veya bağlantı noktası filtreleme aracı uygulayın ve yönetin.	x	x	x	11,2	**Belge Trafiği Yapılandırma Kuralları**		x		x			x

4	4,2	Ağ	Koruma (Protect)	Ağ Altyapısı için Güvenli Bir Yapılandırma Süreci Oluşturun ve Bakımını Yapın	Ağ cihazları için güvenli bir yapılandırma süreci oluşturun ve bakımını yapın. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	11,3	Standart Cihaz Yapılandırmalarını Doğrulamak ve Değişiklikleri Algılamak için Otomatik Araçları Kullanın		x		x		x		
7	7,4	Uygulamalar	Koruma (Protect)	Otomatik Uygulama Yama Yönetimini Gerçekleştirin	Otomatik yama yönetimi aracılığıyla kurumsal varlıklarda uygulama güncellemelerini aylık veya daha sık aralıklarla gerçekleştirin.	x	x	x	11,4	Güvenlikle İlgili Tüm Güncelleştirmelerin En Son Kararlı Sürümünü Tüm Ağ Aygıtlarına Yükleyin		x		x			x	
12	12,1	Ağ	Koruma (Protect)	Ağ Altyapısının Güncel Olduğundan Emin Olun	Ağ altyapısının güncel tutulmasını sağlayın. Örnek uygulamalar, yazılımın en son kararlı sürümünü çalıştırmayı ve/veya şu anda desteklenen hizmet olarak ağ (NaaS) tekliflerini kullanmayı içerir. Yazılım desteğini doğrulamak için yazılım sürümlerini aylık olarak veya daha sık gözden geçirin.	x	x	x	11,4	Güvenlikle İlgili Tüm Güncelleştirmelerin En Son Kararlı Sürümünü Tüm Ağ Aygıtlarına Yükleyin	x						x	
12	12,3	Ağ	Koruma (Protect)	Ağ Altyapısını Güvenli Bir Şekilde Yönetin	Ağ altyapısını güvenli bir şekilde yönetin. Örnek uygulamalar, sürüm kontrollü kod olarak altyapıyı ve SSH ve HTTPS gibi güvenli ağ protokollerinin kullanımını içerir.		x	x	11,5	Çok Faktörlü Kimlik Doğrulama ve Şifreli Oturumlar Kullanarak Ağ Cihazlarını Yönetin	x							x
12	12,8	Cihazlar	Koruma (Protect)	Tüm Yönetici İşler için Özel Bilgi İşlem Kaynakları Oluşturun ve Bakımını Yapın	Tüm yönetici görevler veya yönetici erişim gerektiren görevler için fiziksel veya mantıksal olarak ayrılmış özel bilgi işlem kaynakları oluşturun ve yedeğini alın. Bilgi işlem kaynakları, işletmenin birincil ağından bölümlere ayrılmalı ve internet erişimine izin verilmemelidir.			x	11,6	Tüm Ağ Yönetim Görevleri için Özel İş İstasyonlarını Kullanın	x			x		x		
12	12,8	Cihazlar	Koruma (Protect)	Tüm Yönetici İşler için Özel Bilgi İşlem Kaynakları Oluşturun ve Bakımını Yapın	Tüm yönetici görevler veya yönetici erişim gerektiren görevler için fiziksel veya mantıksal olarak ayrılmış özel bilgi işlem kaynakları oluşturun ve sürdürün. Bilgi işlem kaynakları, işletmenin birincil ağından bölümlere ayrılmalı ve internet erişimine izin verilmemelidir.			x	11,7	Özel Bir Ağ Üzerinden Ağ Altyapısını Yönetin	x			x		x		
12	12,4	Ağ	Tanımla (Identify)	Mimari Diyagram(lar)ın Oluşturulması ve Yedeğini Alın	Mimari şemaları ve/veya diğer ağ sistemi belgelerini oluşturun ve sürdürün. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.		x	x	12,1	Ağ Sınırlarının Envanterini Koruyun	x					x		
7	7,5	Uygulamalar	Tanımla (Identify)	Dahili Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin	Dahili kurumsal varlıkların otomatik güvenlik açığı taramalarını üç ayda bir veya daha sık aralıklarla gerçekleştirin. SCAP uyumlu bir güvenlik açığı tarama aracı kullanarak hem kimliği doğrulanmış hem de kimliği doğrulanmamış taramalar gerçekleştirin.		x	x	12,2	Güvenilir Ağ Sınırlarında Yetkisiz Bağlantıları Tarayın		x		x			x	
7	7,6	Uygulamalar	Tanımla (Identify)	Dışarıdan Tespit Edilen Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin	SCAP uyumlu bir güvenlik açığı tarama aracı kullanarak harici olarak açığa çıkan kurumsal varlıkların otomatik güvenlik açığı taramalarını gerçekleştirin. Taramaları aylık veya daha sık aralıklarla gerçekleştirin.		x	x	12,2	Güvenilir Ağ Sınırlarında Yetkisiz Bağlantıları Tarayın		x		x			x	
13	13,5	Cihazlar	Koruma (Protect)	Uzak Varlıklar için Erişim Kontrolünü Yönetin	Kurumsal kaynaklara uzaktan bağlanan varlıklar için erişim kontrolünü yönetin.Yüklü güncel kötü amaçlı yazılımdan koruma yazılımı; kuruluşun güvenli yapılandırma süreciyle yapılandırma uyumluluğu; ve işletim sisteminin ve uygulamaların güncel olmasını sağlamaya dayalı olarak kurumsal kaynaklara erişim miktarını belirleyin.		x	x	12,2	Güvenilir Ağ Sınırlarında Yetkisiz Bağlantıları Tarayın	x			x				x
9	9,2	Ağ	Koruma (Protect)	DNS Filtreleme Hizmetlerini Kullanın	Bilinen kötü amaçlı etki alanlarına erişimi engellemek için tüm kurumsal varlıklarda DNS filtreleme hizmetlerini kullanın.	x	x	x	12,3	Bilinen Kötü Amaçlı IP Adresleriyle İletişimi Reddet		x		x	x			
4	4,4	Cihazlar	Koruma (Protect)	Sunucularda Güvenlik Duvarı Uygulayın ve Yönetin	Desteklendiği yerlerde sunucularda bir güvenlik duvarı uygulayın ve yönetin. Örnek uygulamalar arasında sanal bir güvenlik duvarı, işletim sistemi güvenlik duvarı veya bir üçüncü taraf güvenlik duvarı aracısı bulunur.	x	x	x	12,4	Yetkisiz Bağlantı Noktaları Üzerinden İletişimi Reddet		x		x			x	
4	4,5	Cihazlar	Koruma (Protect)	Son Kullanıcı Cihazlarında Güvenlik Duvarı Uygulama ve Yönetme	Açıkça izin verilen hizmetler ve bağlantı noktaları dışındaki tüm trafiği bırakan bir varsayılan reddet kuralı yla, son kullanıcı cihazlarında ana bilgisayar tabanlı bir güvenlik duvarı veya bağlantı noktası filtreleme aracı uygulayın ve yönetin.	x	x	x	12,4	Yetkisiz Bağlantı Noktaları Üzerinden İletişimi Reddet		x		x			x	
13	13,3	Ağ	Tespit et (Detect)	Ağa İzinsiz Giriş Tespit Çözümü Dağıtın	Uygun olduğunda, kurumsal varlıklara bir ağ saldırı tespit çözümü dağıtın. Örnek uygulamalar, bir Ağ İzinsiz Giriş Tespit Sistemi (NIDS) veya eşdeğer bulut hizmeti sağlayıcısı (CSP) hizmetinin kullanımını içerir.		x	x	12,6	Ağ Tabanlı IDS Sensörlerini Dağıtın	x							x
13	13,8	Ağ	Koruma (Protect)	Ağa İzinsiz Girişi Önleme Çözümü Dağıtın	Uygun olduğunda, bir ağa izinsiz giriş önleme çözümü dağıtın. Örnek uygulamalar, bir Ağa İzinsiz Girişi Önleme Sistemi (NIPS) veya eşdeğer CSP hizmetinin kullanımını içerir.			x	12,7	Ağ Tabanlı Saldırı Önleme Sistemleri Dağıtın	x			x				x
13	13,6	Ağ	Tespit et (Detect)	Ağ Trafiği Akış Günlüklerini(logs) Toplayın	Gözden geçirmek ve ağ cihazlarından uyarı almak için ağ trafiği akış günlüklerini ve/veya ağ trafiğini toplayın.		x	x	12,8	NetFlow Collection'ı Ağ Bağlantısı Sınır Cihazlarına Dağıtın	x							x
13	13,10	Ağ	Koruma (Protect)	Uygulama Katmanı Filtreleme Gerçekleştirin	Uygulama katmanı filtrelemesi gerçekleştirin. Örnek uygulamalar arasında bir filtreleme proxy'si, uygulama katmanı güvenlik duvarı veya ağ geçidi bulunur.			x	12,9	Uygulama Katmanı Filtreleme Proxy Sunucusunu Dağıt	x			x				x
6	6,4	Kullanıcılar	Koruma (Protect)	Uzaktan Ağ Erişimi için MFA Gerektirir	Uzaktan Ağ Erişimi için MFA Gerektirir	x	x	x	12,11	Tüm Uzaktan Oturum Açmaların Çok Faktörlü Kimlik Doğrulamayı Kullanmasını Gerektirin		x						x
13	13,5	Cihazlar	Koruma (Protect)	Uzak Varlıklar için Erişim Kontrolünü Yönetin	Kurumsal kaynaklara uzaktan bağlanan varlıklar için erişim kontrolünü yönetin. Şunlara dayalı olarak kurumsal kaynaklara erişim miktarını belirleyin: yüklü güncel kötü amaçlı yazılımdan koruma yazılımı, kuruluşun güvenli yapılandırma süreciyle yapılandırma uyumluluğu ve işletim sistemi ve uygulamaların güncel olduğundan emin olun.		x	x	12,12	Dahili Ağda Oturum Açan Tüm Cihazları Uzaktan Yönetin	x			x	x			
3	3,2	Veri	Tanımla (Identify)	Bir Veri Envanteri Oluşturun ve Bakımını Yapın	Kuruluşun veri yönetimi sürecine dayalı olarak bir veri envanteri oluşturun ve bakımını yapın. En azından envantere duyarlı veriler. Envanteri, hassas verilere öncelik vererek, en azından yıllık olarak gözden geçirin ve güncelleyin.	x	x	x	13,1	Hassas Bilgi Envanterini Koruyun	x							x
3	3,5	Veri	Koruma (Protect)	Verilerin Güvenli Bir Şekilde İmha Edilmesi	Verileri, kurumun veri yönetimi sürecinde belirtildiği şekilde güvenli bir şekilde elden çıkarın. Bertaraf süreci ve yönteminin veri hassasiyetiyle orantılı olduğundan emin olun.	x	x	x	13,2	Kuruluş Tarafından Düzenli Olarak Erişilmeyen Hassas Verileri veya Sistemleri Kaldırın				x				x
3	3,13	Veri	Koruma (Protect)	Bir Veri Kaybını Önleme Çözümü Dağıtın	Yerinde veya uzak bir hizmet sağlayıcısında bulunanlar da dahil olmak üzere kurumsal varlıklar aracılığıyla depolanan, işlenen veya iletilen tüm hassas verileri belirlemek için ana bilgisayar tabanlı Veri Kaybını Önleme (DLP) aracı gibi otomatik bir araç uygulayın ve işletmenin hassas veri envanterini güncelleyin.			x	13,3	Yetkisiz Ağ Trafiğini İzleyin ve Engelleyin	x			x				x
2	2,3	Uygulamalar	Cevapla (Respond)	Yetkisiz Yazılımı Adresleyin	Yetkisiz yazılımın kurumsal varlıklarda kullanımdan kaldırıldığından veya belgelenmiş bir istisna aldığından emin olun. Aylık veya daha sık gözden geçirin.	x	x	x	13,4	Yalnızca Yetkili Bulut Depolama veya E-posta Sağlayıcılarına Erişime İzin Verin		x		x	x			
9	9,3	Ağ	Koruma (Protect)	Ağ Tabanlı URL Filtrelerini Koruyun ve Uygulayın	Bir kurumsal varlığın potansiyel olarak kötü amaçlı veya onaylanmamış web sitelerine bağlanmasını sınırlamak için ağ tabanlı URL filtrelerini zorunlu kılın ve güncelleyin. Örnek uygulamalar, kategori tabanlı filtrelemeyi, itibar tabanlı filtrelemeyi veya engelleme listelerinin kullanımını içerir. Tüm kurumsal varlıklar için filtreler uygulayın.		x	x	13,4	Yalnızca Yetkili Bulut Depolama veya E-posta Sağlayıcılarına Erişime İzin Verin		x		x	x			
3	3,6	Cihazlar	Koruma (Protect)	Son Kullanıcı Cihazlarındaki Verileri Şifreleyin	Hassas veriler içeren son kullanıcı cihazlarındaki verileri şifreleyin. Örnek uygulamalar arasında Windows BitLocker®, Apple FileVault®, Linux® dm-crypt sayılabilir.	x	x	x	13,6	Mobil Cihaz Verilerini Şifrele	x					x		
3	3,9	Veri	Koruma (Protect)	Çıkarılabilir Medyadaki Verileri Şifrele	Çıkarılabilir ortamdaki verileri şifreleyin.		x	x	13,7	USB Cihazlarını Yönet	x			x				x
3	3,9	Veri	Koruma (Protect)	Çıkarılabilir Medyadaki Verileri Şifrele	Çıkarılabilir ortamdaki verileri şifreleyin.		x	x	13,9	USB Depolama Aygıtlarındaki Verileri Şifreleyin	x			x	x			
3	3,12	Ağ	Protect	Hassasiyete Dayalı Segment Veri İşleme ve Depolama	Verilerin hassasiyetine göre veri işleme ve depolamayı bölümlere ayırın. Daha düşük hassasiyetli verilere yönelik kurumsal varlıklardaki hassas verileri işlemeyin.		x	x	14,1	Ağı Duyarlılığa Göre Segmentlere Ayırın		x		x				x
13	13,4	Ağ	Koruma (Protect)	Ağ Segmentleri Arasında Trafik Filtreleme Gerçekleştirin	Uygun olduğunda, ağ segmentleri arasında trafik filtrelemesi gerçekleştirin.		x	x	14,2	VLAN'lar Arasında Güvenlik Duvarı Filtrelemeyi Etkinleştir		x						x
4	4,1	Uygulamalar	Koruma (Protect)	Güvenli Bir Yapılandırma Süreci Oluşturun ve Sürdürün	Kurumsal varlıklar (taşınabilir ve mobil dahil son kullanıcı cihazları; bilgi işlem dışı/IoT cihazları ve sunucular) ve yazılımlar (işletim sistemleri ve uygulamaları) için güvenli bir yapılandırma süreci oluşturun ve sürdürün. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	14,3	İş İstasyonundan iş İstasyonuna İletişimi devre dışı bırakın		x		x	x			
3	3,10	Veri	Koruma (Protect)	Geçiş Halindeki Hassas Verileri Şifreleyin	Aktarılan hassas verileri şifreleyin. Örnek uygulamalar arasında Aktarım Katmanı Güvenliği (TLS) ve Açık Güvenli Kabuk (OpenSSH) yer alabilir.		x	x	14,4	Geçiş Halindeki Tüm Hassas Bilgileri Şifreleyin		x		x				x
3	3,13	Veri	Koruma (Protect)	Bir Veri Kaybını Önleme Çözümü Dağıtın	Yerinde veya uzak bir hizmet sağlayıcısında bulunanlar da dahil olmak üzere kurumsal varlıklar aracılığıyla depolanan, işlenen veya iletilen tüm hassas verileri belirlemek için ana bilgisayar tabanlı Veri Kaybını Önleme (DLP) aracı gibi otomatik bir araç uygulayın ve işletmenin hassas veri envanterini güncelleyin.			x	14,5	Hassas Verileri Tanımlamak için Aktif Keşif Aracını Kullanın		x		x				x
3	3,3	Veri	Koruma (Protect)	Veri Erişim Kontrol Listelerini Yapılandırın	Bir kullanıcının bilme ihtiyacına göre veri erişim kontrol listelerini yapılandırın. Erişim izinleri olarak da bilinen veri erişim kontrol listelerini yerel ve uzak dosya sistemlerine, veritabanlarına ve uygulamalara uygulayın.	x	x	x	14,6	Erişim Kontrol Listeleri ile Bilgileri Koruyun		x						x
3	3,13	Veri	Koruma (Protect)	Bir Veri Kaybını Önleme Çözümü Dağıtın	Yerinde veya uzak bir hizmet sağlayıcısında bulunanlar da dahil olmak üzere kurumsal varlıklar aracılığıyla depolanan, işlenen veya iletilen tüm hassas verileri belirlemek için ana bilgisayar tabanlı Veri Kaybını Önleme (DLP) aracı gibi otomatik bir araç uygulayın ve işletmenin hassas veri envanterini güncelleyin.			x	14,7	Otomatik Araçlar Aracılığıyla Verilere Erişim Denetimini Zorlayın		x		x				x
3	3,11	Veri	Koruma (Protect)	Bekleyen(rest) Hassas Verileri Şifreleyin	Hassas verileri içeren sunucularda, uygulamalarda ve veritabanlarında bekleyen hassas verileri şifreleyin. Sunucu tarafı şifreleme olarak da bilinen depolama katmanı şifrelemesi, bu Korumanın minimum gereksinimini karşılar. Ek şifreleme yöntemleri, veri depolama aygıtına/cihazlarına erişimin düz metin verilerine erişime izin vermediği durumlarda, istemci tarafı şifreleme olarak da bilinen uygulama katmanı şifrelemesini içerebilir.		x	x	14,8	Hareketsizken Hassas Bilgileri Şifreleyin		x		x	x			
3	3,14	Veri	Tespit et (Detect)	Günlük(log) Hassas Veri Erişimi	Değişiklik ve imha dahil olmak üzere hassas veri erişimini günlüğe kaydedin.			x	14,9	Hassas Verilere Erişim veya Değişiklikler için Ayrıntı Günlüğünü Zorlayın		x						x
1	1,1	Cihazlar	Tanımla (Identify)	Ayrıntılı Kurumsal Varlık Envanteri Oluşturun ve Bakımını Yapın	Son kullanıcı cihazları (taşınabilir ve mobil dahil), ağ cihazları, bilgi işlem dışı/IoT cihazları ve sunucuları içerecek şekilde, verileri depolama veya işleme potansiyeline sahip tüm kurumsal varlıkların doğru, ayrıntılı ve güncel bir envanterini oluşturun ve yedeğini alın.Envanterin ağ adresini (statikse), donanım adresini, makine adını, veri varlığı sahibini, her varlık için departmanını ve varlığın ağa bağlanmak için onaylanıp onaylanmadığını kaydettiğinden emin olun. Mobil son kullanıcı cihazları için, uygun olduğunda MDM türü araçlar bu süreci destekleyebilir. Bu envanter, fiziksel, sanal, uzaktan altyapıya bağlı ve bulut ortamlarındaki varlıkları içerir. Ek olarak, kuruluşun kontrolü altında olmasalar bile kuruluşun ağ altyapısına düzenli olarak bağlanan varlıkları içerir. Tüm kurumsal varlıkların envanterini iki yılda bir veya daha sık gözden geçirin ve güncelleyin.	x	x	x	15,1	Yetkili Kablosuz Erişim Noktalarının Envanterini Tutun		x		x	x			
1	1,5	Cihazlar	Tespit et (Detect)	Pasif Varlık Keşif Aracı kullanın	Kuruluşun ağına bağlı varlıkları belirlemek için pasif bir keşif aracı kullanın. Kuruluşun varlık envanterini en az haftada bir veya daha sık güncellemek için taramaları gözden geçirin ve kullanın.			x	15,2	Kablolu Ağa Bağlı Kablosuz Erişim Noktalarını Algıla		x		x		x		
13	13,8	Ağ	Koruma (Protect)	Ağa İzinsiz Girişi Önleme Çözümü Dağıtın	Uygun olduğunda, bir ağa izinsiz giriş önleme çözümü dağıtın. Örnek uygulamalar, bir Ağa İzinsiz Giriş Önleme Sistemi (NIPS) veya eşdeğer CSP hizmetinin kullanımını içerir.			x	15,3	Kablosuz İzinsiz Giriş Tespit Sistemi Kullanın		x		x		x		
4	4,8	Cihazlar	Koruma (Protect)	Kurumsal Varlıklar ve Uygulamalarda Gereksiz Hizmetleri Kaldırın veya Devre Dışı Bırakın	Kullanılmayan dosya paylaşım hizmeti, web uygulama modülü veya hizmet işlevi gibi kurumsal varlıklar ve yazılımlardaki gereksiz hizmetleri kaldırın veya devre dışı bırakın.		x	x	15,4	Gerekli Değilse Cihazlarda Kablosuz Erişimi Devre Dışı Bırakın		x		x	x			
4	4,8	Cihazlar	Koruma (Protect)	Kurumsal Varlıklar ve Yazılımlarda Gereksiz Hizmetleri Kaldırın veya Devre Dışı Bırakın	Kullanılmayan dosya paylaşım hizmeti, web uygulama modülü veya hizmet işlevi gibi kurumsal varlıklar ve yazılımlardaki gereksiz hizmetleri kaldırın veya devre dışı bırakın.		x	x	15,6	Kablosuz İstemcilerde Eşler Arası Kablosuz Ağ Özelliklerini Devre Dışı Bırakın		x		x				x
3	3,10	Veri	Koruma (Protect)	Geçiş Halindeki Hassas Verileri Şifreleyin	Aktarılan hassas verileri şifreleyin. Örnek uygulamalar arasında Aktarım Katmanı Güvenliği (TLS) ve Açık Güvenli Kabuk (OpenSSH) yer alabilir.		x	x	15,7	Kablosuz Verileri Şifrelemek için Gelişmiş Şifreleme Standardından (AES) yararlanın		x		x		x		
12	12,6	Ağ	Koruma (Protect)	Güvenli Ağ Yönetimi ve İletişim Protokollerinin Kullanımı	Güvenli ağ yönetimi ve iletişim protokollerini kullanın (ör. 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise veya üstü).		x	x	15,8	Karşılıklı, Çok Faktörlü Kimlik Doğrulama Gerektiren Kablosuz Kimlik Doğrulama Protokollerini Kullanın		x		x	x			

4	4,8	Cihazlar	Koruma (Protect)	Kurumsal Varlıklar ve Uygulamalarda Gereksiz Hizmetleri Kaldırın veya Devre Dışı Bırakın	Kullanılmayan dosya paylaşım hizmeti, web uygulama modülü veya hizmet işlevi gibi kurumsal varlıklar ve yazılımlardaki gereksiz hizmetleri kaldırın veya devre dışı bırakın.		x	x	15,9	**Cihazların Kablosuz Çevresel Erişimini Devre Dışı Bırak**		x		x			x
12	12,2	Ağ	Koruma (Protect)	Güvenli Bir Ağ Mimarisi Oluşturun ve Bakımını Yapın	Güvenli bir ağ mimarisi oluşturun ve sürdürün. Güvenli bir ağ mimarisi, en azından segmentasyon, en az ayrıcalık ve kullanılabilirliği ele almalıdır.		x	x	15,10	**Kişisel ve Güvenilmeyen Cihazlar için Ayrı Kablosuz Ağ Oluşturun**		x				x	
6	6,6	Kullanıcılar	Tanımla (Identify)	Bir Kimlik Doğrulama ve Yetkilendirme Sistemleri Envanteri Oluşturun ve Bakımını Yapın	Yerinde veya bir uzak hizmet sağlayıcısında barındırılanlar da dahil olmak üzere, kuruluşun kimlik doğrulama ve yetkilendirme sistemlerinin bir envanterini oluşturun ve sürdürün. Envanteri en azından yıllık olarak veya daha sık olarak gözden geçirin ve güncelleyin.		x	x	16,1	**Kimlik Doğrulama Sistemleri Envanterini Koruyun**		x					x
5	5,6	Kullanıcılar	Koruma (Protect)	Hesap Yönetimini Merkezileştirin	Bir dizin veya kimlik hizmeti aracılığıyla hesap yönetimini merkezileştirin.		x	x	16,2	**Merkezi Kimlik Doğrulama Noktasını Yapılandırın**		x					x
6	6,3	Kullanıcılar	Koruma (Protect)	Harici Olarak Açıklanan Uygulamalar için MFA Gerekir	Destekleniyorsa, harici olarak açığa çıkan tüm kurumsal veya üçüncü taraf uygulamalarının MFA'yı zorlamasını zorunlu kılın. MFA'yı bir rehber hizmeti veya SSO sağlayıcısı aracılığıyla uygulamak, bu Korumanın tatmin edici bir uygulamasıdır.	x	x	x	16,3	**Çok Faktörlü Kimlik Doğrulama Gerektir**		x		x	x		
3	3,11	Veri	Koruma (Protect)	Hareketsizken Hassas Verileri Şifreleyin	Hassas verileri içeren sunucularda, uygulamalarda ve veritabanlarında bekleyen hassas verileri şifreleyin. Sunucu tarafı şifreleme olarak da bilinen depolama katmanı şifrelemesi, bu Korumanın minimum gereksinimini karşılar. Ek şifreleme yöntemleri, veri depolama aygıtına/cihazlarına erişimin düz metin verilerine erişime izin vermediği durumlarda, istemci tarafı şifreleme olarak da bilinen uygulama katmanı şifrelemesini içerebilir.		x	x	16,4	**Tüm Kimlik Doğrulama Bilgilerini Şifrele veya Hash Et**		x		x			x
3	3,10	Veri	Koruma (Protect)	Geçiş Halindeki Hassas Verileri Şifreleyin	Aktarılan hassas verileri şifreleyin. Örnek uygulamalar arasında Aktarım Katmanı Güvenliği (TLS) ve Açık Güvenli Kabuk (OpenSSH) yer alabilir.		x	x	16,5	**Kullanıcı Adı ve Kimlik Doğrulama Kimlik Bilgilerinin İletilmesini Şifreleyin**		x		x			x
5	5,1	Kullanıcılar	Tanımla (Identify)	Bir Hesap Envanteri Oluşturun ve Bakımını Yapın	Kuruluşta yönetilen tüm hesapların bir envanterini oluşturun ve yedeğini alın. Envanter hem kullanıcı hem de yönetici hesaplarını içermelidir. Envanter en azından kişinin adını, kullanıcı adını, başlangıç/bitiş tarihlerini ve departmanını içermelidir. Tüm aktif hesapların, en az üç ayda bir veya daha sık aralıklarla yinelenen bir programa göre yetkilendirildiğini doğrulayın.	x	x	x	16,6	**Bir Hesap Envanteri Tutmak**		x		x	x		
6	6,2	Kullanıcılar	Koruma (Protect)	Bir Erişim İptal İşlemi Oluşturun	Bir kullanıcının feshi, haklarının iptali veya rol değişikliğinin hemen ardından hesapları devre dışı bırakarak, kurumsal varlıklara erişimi iptal etmek için tercihen otomatikleştirilmiş bir süreç oluşturun ve izleyin. Denetim izlerini korumak için hesapları silmek yerine hesapları devre dışı bırakmak gerekli olabilir.	x	x	x	16,7	**Erişimi İptal Etme Süreci Oluşturun**		x					
5	5,3	Kullanıcılar	Cevapla (Respond)	Hareketsiz Hesapları Devre Dışı Bırak	Destekleniyorsa, 45 günlük bir hareketsizlik süresinden sonra tüm aktif olmayan hesapları silin veya devre dışı bırakın.	x	x	x	16,8	**İlişkilendirilmemiş Hesapları Devre Dışı Bırak**		x		x			x
5	5,3	Kullanıcılar	Cevapla (Respond)	Hareketsiz Hesapları Devre Dışı Bırak	Destekleniyorsa, 45 günlük bir hareketsizlik süresinden sonra tüm aktif olmayan hesapları silin veya devre dışı bırakın.	x	x	x	16,9	**Hareketsiz Hesapları Devre Dışı Bırak**		x		x			x
5	5,3	Kullanıcılar	Cevapla (Respond)	Hareketsiz Hesapları Devre Dışı Bırak	Destekleniyorsa, 45 günlük bir hareketsizlik süresinden sonra tüm aktif olmayan hesapları silin veya devre dışı bırakın.	x	x	x	16,10	**Tüm Hesapların Son Kullanma Tarihine Sahip Olduğundan Emin Olun**		x		x	x		
4	4,3	Kullanıcılar	Koruma (Protect)	Kurumsal Varlıklarda Otomatik Oturum Kilitlemeyi Yapılandırın	Tanımlanmış bir etkinlik dışı kalma süresinden sonra kurumsal varlıklarda otomatik oturum kilitlemeyi yapılandırın. Genel amaçlı işletim sistemlerinde süre 15 dakikayı geçmemelidir. Mobil son kullanıcı cihazlarında süre 2 dakikayı geçmemelidir.	x	x	x	16,11	**Hareketsizlikten Sonra İş İstasyonu Oturumlarını Kilitle**		x					x
8	8,5	Ağ	Tespit et (Detect)	Ayrıntılı Denetim Günlüklerini Toplayın	Hassas veriler içeren kurumsal varlıklar için ayrıntılı denetim günlüğünü yapılandırın. Adli soruşturmaya yardımcı olabilecek olay kaynağı, tarih, kullanıcı adı, zaman damgası, kaynak adresleri, hedef adresleri ve diğer yararlı öğeleri dahil edin.		x	x	16,12	**Devre Dışı Bırakılmış Hesaplara Erişim Girişimlerini İzleme**		x		x			x
14	14,9	N/A	Koruma (Protect)	Role Özgü Güvenlik Bilinci ve Becerileri Eğitimi Gerçekleştirin	Role özel güvenlik farkındalığı ve becerileri eğitimi gerçekleştirin. Örnek uygulamalar arasında BT uzmanları için güvenli sistem yönetimi kursları, (web uygulaması geliştiricileri için OWASP® İlk 10 güvenlik açığı farkındalığı ve önleme eğitimi ve yüksek profilli roller için gelişmiş sosyal mühendislik farkındalık eğitimi yer alır.		x	x	17,2	**Yetenekler Boşluğunu Doldurmak için Eğitim Sunun**	x						x
14	14,1	N/A	Koruma (Protect)	Bir Güvenlik Farkındalık Programı Oluşturun ve Sürdürün	Bir güvenlik bilinci programı oluşturun ve sürdürün. Bir güvenlik bilinci programının amacı, kurumun iş gücünü kurumsal varlıklar ve verilerle güvenli bir şekilde nasıl etkileşime gireceği konusunda eğitmektir. Eğitimi işe alarak ve en azından yıllık olarak gerçekleştirin. İçeriği yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	17,3	**Bir Güvenlik Farkındalık Programı Uygulayın**	x			x			x
14	14,1	N/A	Koruma (Protect)	Bir Güvenlik Farkındalık Programı Oluşturun ve Sürdürün	Bir güvenlik bilinci programı oluşturun ve sürdürün. Bir güvenlik bilinci programının amacı, kurumun iş gücünü kurumsal varlıklar ve verilerle güvenli bir şekilde nasıl etkileşime gireceği konusunda eğitmektir. Eğitimi işe alarak ve en azından yıllık olarak gerçekleştirin. İçeriği yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	17,4	**Farkındalık İçeriğini Sık Sık Güncelleyin**	x			x	x		
14	14,3	N/A	Koruma (Protect)	İş Gücü Üyelerini Kimlik Doğrulama En İyi Uygulamaları konusunda Eğitin	İş gücü üyelerini en iyi kimlik doğrulama uygulamaları konusunda eğitin. Örnek konular arasında MFA, parola oluşturma ve kimlik bilgisi yönetimi yer alır.	x	x	x	17,5	**İş Gücünü Güvenli Kimlik Doğrulama konusunda eğitin**	x						x
14	14,2	N/A	Koruma (Protect)	İş Gücü Üyelerini Sosyal Mühendislik Saldırılarını Tanıyacak Şekilde Eğitin	Kimlik avı, ön mesaj gönderme ve kuyruk kapısı gibi sosyal mühendislik saldırılarını tanımak için iş gücü üyelerini eğitin.	x	x	x	17,6	**İş Gücünü Sosyal Mühendislik Saldırılarını Belirleme Konusunda Eğitin**	x						x
14	14,4	N/A	Koruma (Protect)	İş Gücünü Veri İşleme En İyi Uygulamaları konusunda Eğitin	İş gücü üyelerini hassas verilerin nasıl tanımlanacağı ve uygun şekilde depolanacağı, aktarılacağı, arşivleneceği ve imha edileceği konusunda eğitin. Bu ayrıca, kurumsal varlıklarından uzaklaştıklarında ekranlarını kilitleme, toplantıların sonunda fiziksel ve sanal beyaz tahtaları silme ve veri ve varlıkları güvenli bir şekilde depolama gibi net ekran ve masa üstü en iyi uygulamaları konusunda iş gücü üyelerine eğitim vermeyi içerir.	x	x	x	17,7	**İş Gücünü Hassas Veri İşleme Konusunda Eğitin**	x						x
14	14,5	N/A	Koruma (Protect)	İşgücü Üyelerini Kasıtsız Verilere Maruz Kalma Nedenleri Konusunda Eğitin	İşgücü üyelerini, kasıtsız veri maruziyetinin nedenlerinin farkında olmaları için eğitin. Örnek konular arasında hassas verilerin yanlış teslimi, taşınabilir bir son kullanıcı cihazının kaybolması veya istenmeyen kitlelere veri yayınlanması sayılabilir.	x	x	x	17,8	**İşgücünü Kasıtsız Verilere Maruz Kalmanın Nedenleri Konusunda Eğitin**	x						x
14	14,6	N/A	Koruma (Protect)	Güvenlik Olaylarını Tanıma ve Raporlama konusunda İş Gücü Üyelerini Eğitin	Potansiyel bir olayı fark edebilmek ve böyle bir olayı rapor edebilmek için işgücü üyelerini eğitin.	x	x	x	17,9	**İş Gücü Üyelerini Olayları Tespit Etme ve Rapor Etme Konusunda Eğitin**	x						x
16	16,1	Uygulamalar	Koruma (Protect)	Güvenli Bir Uygulama Geliştirme Süreci Oluşturun ve Sürdürün	Güvenli bir uygulama geliştirme süreci oluşturun ve sürdürün. Bu süreçte, güvenli uygulama tasarım standartları, güvenli kodlama uygulamaları, geliştirici eğitimi, güvenlik açığı yönetimi, üçüncü taraf kodunun güvenliği ve uygulama güvenliği test prosedürleri gibi öğeleri ele alın. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.		x	x	18,1	**Güvenli Kodlama Uygulamaları Oluşturun**	x						x
16	16,10	Uygulamalar	Koruma (Protect)	Uygulama Mimarilerinde Güvenli Tasarım İlkelerini Uygulayın	Uygulama mimarilerinde güvenli tasarım ilkelerini uygulayın. Güvenli tasarım ilkeleri, en az ayrıcalık kavramını ve kullanıcının yaptığı her işlemi doğrulamak için arabuluculuğu zorunlu kılarak "kullanıcı girdisine asla güvenme" kavramını teşvik eder. Örnekler, boyut, veri türü ve kabul edilebilir aralıklar veya biçimler dahil olmak üzere tüm girdiler için açık hata denetiminin gerçekleştirilmesini ve belgelenmesini içerir. Güvenli tasarım ayrıca, korumasız bağlantı noktalarını ve hizmetleri kapatmak, gereksiz programları ve dosyaları kaldırmak ve varsayılan hesapları yeniden adlandırmak veya kaldırmak gibi uygulama altyapısı saldırı yüzeyini en aza indirmek anlamına gelir.		x	x	18,2	**Şirket İçi Geliştirilen Tüm Yazılımlar İçin Açık Hata Kontrolü Yapıldığından Emin Olun**	x			x			x
16	16,4	Uygulamalar	Koruma (Protect)	Üçüncü Taraf Yazılım Bileşenleri Envanterini Oluşturun ve Yönetin	Geliştirmede kullanılan ve genellikle "malzeme listesi" olarak adlandırılan üçüncü taraf bileşenlerinin ve ayrıca gelecekte kullanılmak üzere planlanan bileşenlerin güncellenmiş bir envanterini oluşturun ve yönetin. Bu envanter, her bir üçüncü taraf bileşeninin oluşturabileceği riskleri içerecektir. Bu bileşenlerdeki değişiklikleri veya güncellemeleri belirlemek için listeyi en az ayda bir değerlendirin ve bileşenin hala desteklendiğini doğrulayın.		x	x	18,3	**Satın Alınan Yazılımın Hala Desteklendiğini Doğrulayın**	x			x			x
16	16,5	Uygulamalar	Koruma (Protect)	Güncel ve Güvenilir Üçüncü Taraf Yazılım Bileşenlerini Kullanın	Güncel ve güvenilir üçüncü taraf yazılım bileşenlerini kullanın. Mümkün olduğunda, yeterli güvenlik sağlayan yerleşik ve kanıtlanmış çerçeveler ve kitaplıklar seçin. Bu bileşenleri güvenilir kaynaklardan edinin veya kullanmadan önce yazılımı güvenlik açıkları açısından değerlendirin.		x	x	18,4	**Yalnızca Güncel ve Güvenilir Üçüncü Taraf Bileşenlerini Kullanın**	x				x		
16	16,11	Uygulamalar	Koruma (Protect)	Uygulama Güvenliği Bileşenleri için Kontrol Edilen Modüller veya Hizmetlerden Yararlanın	Kimlik yönetimi, şifreleme ve denetleme ve günlüğe kaydetme gibi uygulama güvenliği bileşenleri için onaylanmış modüllerden veya hizmetlerden yararlanın. Platform özelliklerinin kritik güvenlik işlevlerinde kullanılması, geliştiricilerin iş yükünü azaltacak ve tasarım veya uygulama hataları olasılığını en aza indirecektir. Modern işletim sistemleri, tanımlama, kimlik doğrulama ve yetkilendirme için etkili mekanizmalar sağlar ve bu mekanizmaları uygulamalar için kullanılabilir hale getirir. Yalnızca standartlaştırılmış, şu anda kabul edilmiş ve kapsamlı bir şekilde gözden geçirilmiş şifreleme algoritmalarını kullanın. İşletim sistemleri ayrıca güvenli denetim günlükleri oluşturmak ve sürdürmek için mekanizmalar sağlar.		x	x	18,5	**Yalnızca Standartlaştırılmış ve Kapsamlı Olarak İncelenen Şifreleme Algoritmalarını kullanın**	x			x			x
16	16,9	Uygulamalar	Koruma (Protect)	Geliştiricileri Uygulama Güvenliği Kavramları ve Güvenli Kodlama Konusunda Eğitin	Tüm yazılım geliştirme personelinin, kendi özel geliştirme ortamları ve sorumlulukları için güvenli kod yazma konusunda eğitim almalarını sağlayın. Eğitim, genel güvenlik ilkelerini ve uygulama güvenliği standart uygulamalarını içerebilir. En az yılda bir kez eğitim yapın ve geliştirme ekibi içinde güvenliği teşvik edecek şekilde tasarım yapın ve geliştiriciler arasında bir güvenlik kültürü oluşturun.		x	x	18,6	**Yazılım Geliştirme Personelinin Güvenli Kodlama Eğitimi Almasını Sağlayın**	x						x
16	16,12	Uygulamalar	Koruma (Protect)	Kod Düzeyinde Güvenlik Kontrolleri Uygulayın	Güvenli kodlama uygulamalarının takip edildiğini doğrulamak için uygulama yaşam döngüsü içinde statik ve dinamik analiz araçları uygulayın.			x	18,7	**Statik ve Dinamik Kod Analiz Araçlarını Uygulayın**	x			x		x	
16	16,2	Uygulamalar	Koruma (Protect)	Yazılım Açıklarını Kabul Etmek ve Ele Almak için Bir Süreç Oluşturun ve Sürdürün	Dış varlıkların raporlaması için bir araç sağlamak da dahil olmak üzere, yazılım güvenlik açıklarına ilişkin raporları kabul etmek ve ele almak için bir süreç oluşturun ve sürdürün. Bu süreç şu öğeleri içerecektir: raporlama sürecini tanımlayan bir güvenlik açığı işleme politikası, güvenlik açığı raporlarını işlemekten sorumlu taraf, ve alım, atama, iyileştirme ve iyileştirme testi için bir süreç Sürecin parçası olarak, güvenlik açıklarının tanımlanması, analizi ve düzeltilmesi için zamanlamayı ölçmek için önem dereceleri ve ölçümler içeren bir güvenlik açığı izleme sistemi kullanın. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin. Üçüncü taraf uygulama geliştiricilerinin, bunu dış paydaşlar için beklentileri belirlemeye yardımcı olan, dışa dönük bir politika olarak görmesi gerekir.		x	x	18,8	**Yazılım Açıklarına İlişkin Raporları Kabul Etmek ve Ele Almak için Bir Süreç Oluşturun**							x
16	16,8	Uygulamalar	Koruma (Protect)	Ayrı Üretim ve Üretim Dışı Sistemler	Üretim ve üretim dışı sistemler için ayrı ortamlar sağlayın.		x	x	18,9	**Ayrı Üretim ve Üretim Dışı Sistemler**	x						x
13	13,10	Ağ	Koruma (Protect)	Uygulama Katmanı Filtreleme Gerçekleştirin	Uygulama katmanı filtrelemesi gerçekleştirin. Örnek uygulamalar arasında bir filtreleme proxy'si, uygulama katmanı güvenlik duvarı veya ağ geçidi bulunur.			x	18,10	**Web Uygulaması Güvenlik Duvarlarını Dağıtın**		x		x	x		
16	16,7	Uygulamalar	Koruma (Protect)	Uygulama Altyapısı için Standart Sertleştirme Yapılandırma Şablonlarını Kullanın	Uygulama altyapısı bileşenleri için standart, endüstri tarafından önerilen sağlamlaştırma yapılandırma şablonlarını kullanın. Bu, temel sunucuları, veritabanlarını ve web sunucularını içerir ve bulut kapsayıcıları, Hizmet olarak Platform (PaaS) bileşenleri ve SaaS bileşenleri için geçerlidir. Şirket içinde geliştirilen yazılımın yapılandırma sağlamlaştırmasını zayıflatmasına izin vermeyin.		x	x	18,11	**Veritabanları için Standart Sağlamlaştırma Yapılandırma Şablonlarını Kullanın**	x						x
17	17,4	N/A	Cevapla (Respond)	Bir Olay Müdahale Süreci Oluşturma ve Sürdürme	Rolleri ve sorumlulukları, uyumluluk gereksinimlerini ve bir iletişim planını ele alan bir olay müdahale süreci oluşturun ve sürdürün. Yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin.		x	x	19,1	**Olay Müdahale Prosedürlerini Belgeleyin**	x					x	
17	17,5	N/A	Cevapla (Respond)	Anahtar Rolleri ve Sorumlulukları Atayın	Hukuk, BT, bilgi güvenliği, tesisler, halkla ilişkiler, insan kaynakları, olay müdahale ekipleri ve uygun olduğu şekilde analistlerden oluşan personel de dahil olmak üzere olay müdahalesi için kilit roller ve sorumluluklar atayın. Yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin.		x	x	19,2	**Olay Müdahalesi için İş Unvanları ve Görevleri Atayın**	x						x

17	17,1	N/A	Cevapla (Respond)	Olay Yönetimini Yönetecek Personeli Belirleyin	Kuruluşun olay işleme sürecini yönetecek bir kilit kişi ve en az bir yedek belirleyin. Yönetim personeli, olaya müdahale ve kurtarma çabalarının koordinasyonundan ve belgelenmesinden sorumludur ve kuruluş içindeki çalışanlardan, üçüncü taraf satıcılardan veya hibrit bir yaklaşımdan oluşabilir. Üçüncü taraf bir satıcı kullanıyorsanız, herhangi bir üçüncü taraf çalışmasını denetlemek için kuruluş içinden en az bir kişi atayın. Yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin.	x	x	x	19,3	Olay Yönetimini Destekleyecek Yönetim Personelini Belirleyin	x						x
17	17,3	N/A	Cevapla (Respond)	Olayları Raporlamak için bir Kurumsal Süreç Oluşturma ve Sürdürme	İş gücünün güvenlik olaylarını bildirmesi için bir kurumsal süreç oluşturun ve sürdürün. Süreç, raporlama zaman çerçevesini, rapor edilecek personeli, raporlama mekanizmasını ve rapor edilecek minimum bilgiyi içerir. Sürecin tüm işgücü için kamuya açık olduğundan emin olun. Yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin.	x	x	x	19,4	Olayları Raporlamak için Kuruluş Çapında Standartlar Oluşturun	x			x			x
17	17,2	N/A	Cevapla (Respond)	Güvenlik Olaylarını Bildirmek için İletişim Bilgilerini Oluşturun ve Koruyun	Güvenlik olayları hakkında bilgilendirilmesi gereken taraflar için iletişim bilgilerini oluşturun ve sürdürün. İlgili kişiler, dahili personel, üçüncü taraf satıcılar, kolluk kuvvetleri, siber sigorta sağlayıcıları, ilgili devlet kurumları, Bilgi Paylaşımı ve Analiz Merkezi (ISAC) ortakları veya diğer paydaşları içerebilir. Bilgilerin güncel olduğundan emin olmak için kişileri yıllık olarak doğrulayın.	x	x	x	19,5	Güvenlik Olaylarını Bildirmek İçin İletişim Bilgilerini Koruyun	x						x
17	17,3	N/A	Cevapla (Respond)	Olayları Raporlamak için bir Kurumsal Süreç Oluşturma ve Sürdürme	İş gücünün güvenlik olaylarını bildirmesi için bir kurumsal süreç oluşturun ve sürdürün. Süreç, raporlama zaman çerçevesini, rapor edilecek personeli, raporlama mekanizmasını ve rapor edilecek minimum bilgiyi içerir. Sürecin tüm işgücü için kamuya açık olduğundan emin olun. Yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin.	x	x	x	19,6	Bilgisayar Anomalilerini ve Olaylarını Raporlamayla İlgili Bilgileri Yayınlayın	x			x		x	
17	17,7	N/A	Kurtarma (Recover)	Rutin Olay Müdahale Tatbikatları Yapın	Gerçek dünyadaki olaylara müdahale etmeye hazırlanmak için olay müdahale sürecine dahil olan kilit personel için rutin olay müdahale tatbikatları ve senaryoları planlayın ve yürütün. Alıştırmaların iletişim kanallarını, karar vermeyi ve iş akışlarını test etmesi gerekir. En azından yıllık bazda testler yapın.		x	x	19,7	Personel için Periyodik Olay Senaryosu Oturumları Gerçekleştirin	x						x
17	17,9	N/A	Kurtarma (Recover)	Güvenlik Olayı Eşiklerini Oluşturun ve Koruyun	Asgari olarak bir olay ve bir olay arasında ayrım yapmak dahil olmak üzere güvenlik olayı eşiklerini oluşturun ve sürdürün. Örnekler şunları içerebilir: anormal etkinlik, güvenlik açığı, güvenlik zayıflığı, veri ihlali, gizlilik olayı vb. Yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin.			x	19,8	Olay Puanlaması ve Önceliklendirme Şeması Oluşturun	x						x
18	18,1	N/A	Tanımla (Identify)	Bir Sızma Testi Programı Oluşturun ve Sürdürün	İşletmenin büyüklüğüne, karmaşıklığına ve olgunluğuna uygun bir sızma testi programı oluşturun ve sürdürün. Sızma testi ağ, web uygulaması, Uygulama Programlama Arayüzü (API), barındırılan hizmetler ve fiziksel öncül kontrolleri ; Sıklık; kabul edilebilir saatler ve hariç tutulan saldırı türleri gibi sınırlamalar; iletişim noktası bilgileri; bulguların dahili olarak nasıl yönlendirileceği gibi iyileştirme; ve geriye dönük gereksinimler gibi program özelliklerini kapsar.		x	x	20,1	Bir Sızma Testi Programı Oluşturun	x						x
18	18,2	Ağ	Tanımla (Identify)	Periyodik Dış Penetrasyon Testleri Gerçekleştirin	En az yılda bir olmak üzere, program gereksinimlerine dayalı olarak periyodik dış sızma testleri gerçekleştirin. Dış sızma testi, sömürülebilir bilgileri tespit etmek için kurumsal ve çevresel keşifleri içermelidir. Penetrasyon testi, özel beceriler ve deneyim gerektirir ve kalifiye bir taraf aracılığıyla gerçekleştirilmelidir. Test şeffaf kutu veya opak kutu olabilir.		x	x	20,2	Düzenli Dış ve İç Penetrasyon Testleri Gerçekleştirin	x			x			x
18	18,5	N/A	Tanımla (Identify)	Periyodik İç Penetrasyon Testleri Gerçekleştirin	En az yılda bir olmak üzere, program gereksinimlerine dayalı olarak periyodik dahili sızma testleri gerçekleştirin. Test şeffaf kutu veya opak kutu olabilir.			x	20,2	Düzenli Dış ve İç Penetrasyon Testleri Gerçekleştirin	x			x		x	
18	18,2	Ağ	Tanımla (Identify)	Periyodik Dış Penetrasyon Testleri Gerçekleştirin	En az yılda bir olmak üzere, program gereksinimlerine dayalı olarak periyodik dış sızma testleri gerçekleştirin. Dış sızma testi, sömürülebilir bilgileri tespit etmek için kurumsal ve çevresel keşifleri içermelidir. Penetrasyon testi, özel beceriler ve deneyim gerektirir ve kalifiye bir taraf aracılığıyla gerçekleştirilmelidir. Test şeffaf kutu veya opak kutu olabilir.		x	x	20,3	Periyodik Kırmızı Takım Egzersizleri Yapın	x			x	x		
18	18,5	N/A	Tanımla (Identify)	Periyodik İç Penetrasyon Testleri Gerçekleştirin	En az yılda bir olmak üzere, program gereksinimlerine dayalı olarak periyodik dahili sızma testleri gerçekleştirin. Test şeffaf kutu veya opak kutu olabilir.			x	20,3	Periyodik Kırmızı Takım Egzersizleri Yapın	x			x			x
18	18,2	Ağ	Tanımla (Identify)	Periyodik Dış Penetrasyon Testleri Gerçekleştirin	En az yılda bir olmak üzere, program gereksinimlerine dayalı olarak periyodik dış sızma testleri gerçekleştirin. Dış sızma testi, sömürülebilir bilgileri tespit etmek için kurumsal ve çevresel keşifleri içermelidir. Penetrasyon testi, özel beceriler ve deneyim gerektirir ve kalifiye bir taraf aracılığıyla gerçekleştirilmelidir. Test şeffaf kutu veya opak kutu olabilir.		x	x	20,4	Korunmayan Sistem Bilgisi ve Artifaktlarının Varlığına Yönelik Testleri Dahil Edin	x			x			x
5	5,5	Kullanıcılar	Tanımla (Identify)	Hizmet Hesapları Envanteri Oluşturun ve Bakımını Yapın	Hizmet hesaplarının bir envanterini oluşturun ve sürdürün. Envanter, en azından departman sahibini, gözden geçirme tarihini ve amacını içermelidir. Tüm etkin hesapların yetkilendirildiğini doğrulamak için, en az üç ayda bir veya daha sık aralıklarla yinelenen bir programa göre hizmet hesabı incelemeleri gerçekleştirin.		x	x	20,8	Penetrasyon Testiyle İlişkili Hesapları Kontrol Etme ve İzleme		x		x			x
3	3,1	Veri	Tanımla (Identify)	Bir Veri Yönetim Süreci Oluşturma ve Sürdürme	Bir veri yönetimi süreci oluşturun ve sürdürün. Süreçte, kurum için hassasiyet ve saklama standartlarına dayalı olarak veri hassasiyetini, veri sahibini, verilerin işlenmesini, veri saklama limitlerini ve elden çıkarma gereksinimlerini ele alın. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	New				x				
3	3,4	Veri	Koruma (Protect)	Veri Tutmayı Zorunlu Kıl	Verileri, kurumun veri yönetimi sürecine göre saklayın. Veri saklama hem minimum hem de maksimum zaman çizelgelerini içermelidir.	x	x	x	New				x				
3	3,5	Veri	Koruma (Protect)	Verilerin Güvenli Bir Şekilde İmha Edilmesi	Verileri, kurumun veri yönetimi sürecinde belirtildiği şekilde güvenli bir şekilde elden çıkarın. Bertaraf süreci ve yönteminin veri hassasiyetiyle orantılı olduğundan emin olun.	x	x	x	New				x				
3	3,7	Veri	Tanımla (Identify)	Bir Veri Sınıflandırma Planı Oluşturun ve Sürdürün	Kuruluş için genel bir veri sınıflandırma şeması oluşturun ve sürdürün. İşletmeler, “Hassas”, “Gizli” ve “Genel” gibi etiketler kullanabilir ve verilerini bu etiketlere göre sınıflandırabilir. Sınıflandırma şeması yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.		x	x	New				x				
3	3,8	Veri	Tanımla (Identify)	Belge Veri Akışları	Belge veri akışları. Veri akışı belgeleri, hizmet sağlayıcı veri akışlarını içerir ve kuruluşun veri yönetimi sürecini temel almalıdır. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.		x	x	New				x				
4	4,6	Ağ	Koruma (Protect)	Kurumsal Varlıkları ve Yazılımları Güvenle Yönetin	Kurumsal varlıkları ve yazılımları güvenli bir şekilde yönetin. Örnek uygulamalar, sürüm kontrollü kod olarak altyapı aracılığıyla yapılandırmayı yönetmeyi ve Güvenli Kabuk (SSH) ve Güvenli Köprü Metni Aktarım Protokolü (HTTPS) gibi güvenli ağ protokolleri üzerinden yönetici arabirimlerine erişmeyi içerir. Operasyonel olarak gerekli olmadıkça Telnet (Teletype Network) ve HTTP gibi güvenli olmayan yönetim protokollerini kullanmayın.	x	x	x	New				x				
4	4,8	Cihazlar	Koruma (Protect)	Kurumsal Varlıklar ve Uygulamalarda Gereksiz Hizmetleri Kaldırın veya Devre Dışı Bırakın	Kullanılmayan dosya paylaşım hizmeti, web uygulama modülü veya hizmet işlevi gibi kurumsal varlıklar ve yazılımlardaki gereksiz hizmetleri kaldırın veya devre dışı bırakın.		x	x	New				x				
4	4,9	Cihazlar	Koruma (Protect)	Kurumsal Varlıklarda Güvenilir DNS Sunucularını Yapılandırın	Kurumsal varlıklarda güvenilir DNS sunucularını yapılandırın. Örnek uygulamalar şunları içerir: varlıkları kurumsal kontrollü DNS sunucularını ve/veya dışarıdan erişilebilen saygın DNS sunucularını kullanacak şekilde yapılandırma.		x	x	New				x				
4	4,10	Cihazlar	Cevapla (Respond)	Taşınabilir Son Kullanıcı Cihazlarında Otomatik Cihaz Kilitlemeyi Zorunlu Kıl	Desteklendiği yerde, taşınabilir son kullanıcı cihazlarında önceden belirlenmiş bir yerel başarısız kimlik doğrulama girişimi eşiğinin ardından otomatik cihaz kilitlemesini uygulayın. Düzüstü bilgisayarlar için 20'den fazla başarısız kimlik doğrulama girişimine izin vermeyin; tabletler ve akıllı telefonlar için en fazla 10 başarısız kimlik doğrulama girişimi. Örnek uygulamalar arasında Microsoft® InTune Cihaz Kilidi ve Apple® Yapılandırma Profili maxFailedAttempts bulunur.		x	x	New				x				
4	4,11	Cihazlar	Koruma (Protect)	Taşınabilir Son Kullanıcı Cihazlarında Uzaktan Silme Özelliğini Zorunlu Kılın	Kayıp veya çalıntı cihazlar gibi uygun görüldüğünde veya bir kişi artık kuruluşu desteklemediğinde, kuruluşa ait taşınabilir son kullanıcı cihazlarından kurumsal verileri uzaktan silin.		x	x	New				x				
4	4,12	Cihazlar	Koruma (Protect)	Mobil Son Kullanıcı Cihazlarında Ayrı Kurumsal Çalışma Alanları	Desteklendiğinde, mobil son kullanıcı cihazlarında ayrı kurumsal çalışma alanlarının kullanıldığından emin olun. Örnek uygulamalar, kurumsal uygulamaları ve verileri kişisel uygulamalardan ve verilerden ayırmak için bir Apple® Konfigürasyon Profili veya Android™ İş Profili kullanmayı içerir.			x	New				x				
5	5,5	Kullanıcılar	Tanımla (Identify)	Hizmet Hesapları Envanteri Oluşturun ve Bakımını Yapın	Hizmet hesaplarının bir envanterini oluşturun ve sürdürün. Envanter, en azından departman sahibini, gözden geçirme tarihini ve amacını içermelidir. Tüm etkin hesapların yetkilendirildiğini doğrulamak için, en az üç ayda bir veya daha sık aralıklarla yinelenen bir programda hizmet hesabı incelemeleri gerçekleştirin.		x	x	New				x				
6	6,1	Kullanıcılar	Koruma (Protect)	Bir Erişim Verme Süreci Oluşturun	Yeni işe alım, haklar verilmesi veya bir kullanıcının rol değişikliği üzerine kurumsal varlıklara erişim izni vermek için tercihen otomatikleştirilmiş bir süreç oluşturun ve izleyin.	x	x	x	New				x				
6	6,3	Kullanıcılar	Koruma (Protect)	Harici Olarak Açıklanan Uygulamalar için MFA Gerektirir	Destekleniyorsa, harici olarak açığa çıkan tüm kurumsal veya üçüncü taraf uygulamalarının MFA'yı zorlamasını zorunlu kılın. MFA'yı bir rehber hizmeti veya SSO sağlayıcısı aracılığıyla uygulamak, bu Korumanın tatmin edici bir uygulamasıdır.	x	x	x	New				x				
6	6,7	Kullanıcılar	Koruma (Protect)	Erişim Kontrolünü Merkezileştirin	Desteklendiğinde, bir dizin hizmeti veya SSO sağlayıcısı aracılığıyla tüm kurumsal varlıklar için erişim kontrolünü merkezileştirin.		x	x	New				x				
6	6,8	Veri	Koruma (Protect)	Rol Tabanlı Erişim Kontrolünü Tanımlayın ve Bakımını Yapın	Kuruluş içindeki her bir rolün kendisine verilen görevleri başarıyla yerine getirmesi için gerekli erişim haklarını belirleyerek ve belgeleyerek rol tabanlı erişim kontrolünü tanımlayın ve sürdürün. Tüm ayrıcalıkların yetkilendirildiğini doğrulamak için, en az yılda bir kez veya daha sık aralıklarla yinelenen bir programda kurumsal varlıkların erişim kontrolü incelemelerini gerçekleştirin.			x	New				x				
7	7,1	Uygulamalar	Koruma (Protect)	Bir Güvenlik Açığı Yönetim Süreci Oluşturun ve Sürdürün	Kurumsal varlıklar için belgelenmiş bir güvenlik açığı yönetimi süreci oluşturun ve sürdürün. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	New				x				
7	7,2	Uygulamalar	Cevapla (Respond)	Bir İyileştirme Süreci Oluşturun ve Sürdürün	Aylık veya daha sık gözden geçirmelerle bir iyileştirme sürecinde belgelenen riske dayalı bir iyileştirme stratejisi oluşturun ve sürdürün.	x	x	x	New				x				
7	7,7	Uygulamalar	Cevapla (Respond)	Algılanan Güvenlik Açıklarını Düzeltin	Düzeltme sürecine bağlı olarak aylık veya daha sık aralıklarla süreçler ve araçlar aracılığıyla yazılımda algılanan güvenlik açıklarını giderin.		x	x	New				x				x
8	8,1	Ağ	Koruma (Protect)	Bir Denetim Günlüğü Yönetim Süreci Oluşturma ve Sürdürme	Kuruluşun günlük kaydı gereksinimlerini tanımlayan bir denetim günlüğü yönetim süreci oluşturun ve sürdürün. En azından kurumsal varlıklar için denetim günlüklerinin toplanması, gözden geçirilmesi ve saklanması konularını ele alın. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	New				x				
8	8,10	Ağ	Koruma (Protect)	Denetim Günlüklerini Sakla	En az 90 gün boyunca kurumsal varlıklar genelinde denetim günlüklerini saklayın.		x	x	New				x				
8	8,12	Veri	Tespit et (Detect)	Servis Sağlayıcı Günlüklerini Toplayın	Destekleniyorsa, servis sağlayıcı günlüklerini toplayın. Örnek uygulamalar, kimlik doğrulama ve yetkilendirme olaylarını, veri oluşturma ve elden çıkarma olaylarını ve kullanıcı yönetimi olaylarını toplamayı içerir.			x	New				x				
9	9,7	Ağ	Koruma (Protect)	E-posta Sunucusu Kötü Amaçlı Yazılımdan Koruma Korumalarını Dağıtın ve Bakımını Yapın	E-posta Sunucusu Kötü Amaçlı Yazılımdan Koruma Korumalarını Dağıtın ve Bakımını Yapın			x	New				x				
10	10,1	Cihazlar	Koruma (Protect)	Kötü Amaçlı Yazılımdan Koruma Yazılımını Dağıtın ve Bakımını Yapın	Tüm kurumsal varlıklarda kötü amaçlı yazılımdan koruma yazılımı dağıtın ve bakımını yapın.	x	x	x	New				x				
10	10,7	Cihazlar	Tespit et (Detect)	Davranış Tabanlı Kötü Amaçlı Yazılımdan Koruma Yazılımı Kullanın	Davranış tabanlı kötü amaçlı yazılımdan koruma yazılımı kullanın.		x	x	New				x				
11	11,1	Veri	Kurtarma (Recover)	Bir Veri Kurtarma Süreci Oluşturma ve Sürdürme	Bir veri kurtarma süreci oluşturun ve sürdürün. Bu süreçte, veri kurtarma etkinliklerinin kapsamını, kurtarma önceliklendirmesini ve yedekleme verilerinin güvenliğini ele alın. Belgeleri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	New				x				
12	12,2	Ağ	Koruma (Protect)	Güvenli Bir Ağ Mimarisi Oluşturun ve Sürdürün	Güvenli bir ağ mimarisi oluşturun ve sürdürün. Güvenli bir ağ mimarisi, en azından segmentasyon, en az ayrıcalık ve kullanılabilirliği ele almalıdır.		x	x	New				x				

12	12,5	Ağ	Koruma (Protect)	Ağ Kimlik Doğrulaması, Yetkilendirme ve Denetimi (AAA) Merkezileştirin	Ağı merkezileştirin AAA.		x	x	New				x				
12	12,6	Ağ	Koruma (Protect)	Güvenli Ağ Yönetimi ve İletişim Protokollerinin Kullanımı	Güvenli ağ yönetimi ve iletişim protokolleri kullanın (ör. 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise veya üstü).		x	x	New				x				
12	12,7	Cihazlar	Koruma (Protect)	Uzak Cihazların Bir VPN Kullandığından ve Bir Kuruluşun AAA Altyapısına Bağlandığından Emin Olun	Kullanıcıların, son kullanıcı cihazlarındaki kurumsal kaynaklara erişmeden önce kurumsal olarak yönetilen VPN ve kimlik doğrulama hizmetlerinde kimlik doğrulaması yapmasını zorunlu kılın.		x	x	New				x				
13	13,2	Cihazlar	Tespit et (Detect)	Ana Bilgisayar Tabanlı Saldırı Tespit Çözümü Dağıtın	Uygun olduğunda ve/veya desteklendiğinde kurumsal varlıklara ana bilgisayar tabanlı bir saldırı tespit çözümü dağıtın.		x	x	New				x				
13	13,7	Cihazlar	Koruma (Protect)	Ana Bilgisayar Tabanlı Saldırı Önleme Çözümü Dağıtın	Uygun olduğunda ve/veya desteklendiğinde, kurumsal varlıklara ana bilgisayar tabanlı bir izinsiz giriş önleme çözümü dağıtın. Örnek uygulamalar, bir Uç Nokta Algılama ve Yanıt (EDR) istemcisinin veya ana bilgisayar tabanlı IPS aracısının kullanımını içerir.			x	New				x				
14	14,7	N/A	Koruma (Protect)	İşgücünü Kurumsal Varlıklarında Güvenlik Güncelleştirmelerinin Eksik Olup Olmadığını Belirleme ve Raporlama Konusunda Eğitin	Güncel olmayan yazılım yamalarının veya otomatik süreçler ve araçlardaki herhangi bir arızanın nasıl doğrulanacağını ve raporlanacağını anlamak için işgücünü eğitin. Bu eğitimin bir kısmı, otomatikleştirilmiş süreçler ve araçlardaki herhangi bir arızanın BT personeline bildirilmesini içermelidir.	x	x	x	New				x				
14	14,8	N/A	Koruma (Protect)	İş Gücünü Güvensiz Ağlara Bağlanmanın ve Kurumsal Verileri İletmenin Tehlikeleri Konusunda Eğitin	İş gücü üyelerini, kurumsal faaliyetler için güvenli olmayan ağlara bağlanmanın ve bu ağlar üzerinden veri aktarmanın tehlikeleri konusunda eğitin. Kuruluşun uzaktan çalışanları varsa, eğitim, tüm kullanıcıların ev ağı altyapısını güvenli bir şekilde yapılandırmasını sağlamak için rehberlik içermelidir.	x	x	x	New				x				
15	15,1	N/A	Tanımla (Identify)	Hizmet Sağlayıcıların Envanterini Oluşturun ve Bakımını Yapın	Hizmet sağlayıcıların bir envanterini oluşturun ve sürdürün. Envanter, bilinen tüm hizmet sağlayıcıları listelemek, sınıflandırma(lar)ı dahil etmek ve her bir hizmet sağlayıcı için bir kurumsal irtibat kişisi belirlemek içindir. Envanteri yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.	x	x	x	New				x				
15	15,2	N/A	Tanımla (Identify)	Bir Hizmet Sağlayıcı Yönetim Politikası Oluşturun ve Sürdürün	Bir hizmet sağlayıcı yönetim politikası oluşturun ve sürdürün. Politikanın, hizmet sağlayıcıların sınıflandırılmasını, envanterini, değerlendirilmesini, izlenmesini ve hizmetten çıkarılmasını ele aldığından emin olun. Politikayı yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyin.		x	x	New				x				
15	15,3	N/A	Tanımla (Identify)	Servis Sağlayıcıları Sınıflandırın	Servis sağlayıcıları sınıflandırın. Sınıflandırma değerlendirmesi, veri duyarlılığı, veri hacmi, kullanılabilirlik gereksinimleri, geçerli düzenlemeler, yapısal risk ve azaltılmış risk gibi bir veya daha fazla özelliği içerebilir. Sınıflandırmaları yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde güncelleyin ve gözden geçirin.		x	x	New				x				
15	15,4	N/A	Koruma (Protect)	Hizmet Sağlayıcı Sözleşmelerinin Güvenlik Gereksinimlerini İçerdiğinden Emin Olun	Servis sağlayıcı sözleşmelerinin güvenlik gereksinimlerini içerdiğinden emin olun. Örnek gereksinimler, minimum güvenlik programı gereksinimleri, güvenlik olayı ve/veya veri ihlali bildirimi ve yanıtı, veri şifreleme gereksinimleri ve veri imha taahhütlerini içerebilir. Bu güvenlik gereksinimleri, işletmenin hizmet sağlayıcı yönetim politikasıyla tutarlı olmalıdır. Sözleşmelerin güvenlik gereksinimlerini karşılamadığından emin olmak için hizmet sağlayıcı sözleşmelerini yıllık olarak gözden geçirin.		x	x	New				x				
15	15,5	N/A	Tanımla (Identify)	Hizmet Sağlayıcıları Değerlendirin	Hizmet sağlayıcılarını işletmenin hizmet sağlayıcı yönetimi politikasına uygun olarak değerlendirin. Değerlendirme kapsamı sınıflandırma (lar) a göre değişiklik gösterebilir ve Hizmet Organizasyonu Denetimi 2 (SOC 2) ve Ödeme Kartı Endüstrisi (PCI) Uygunluk Onayı (AoC), özelleştirilmiş anketler veya diğer uygun şekilde titiz süreçler gibi standartlaştırılmış değerlendirme raporlarının gözden geçirilmesini içerebilir. Servis sağlayıcıları yıllık olarak, en azından veya yeni ve yenilenen sözleşmelerle yeniden değerlendirin.			x	New				x				
15	15,6	Veri	Tespit et (Detect)	Servis Sağlayıcıları İzleme	Kuruluşun hizmet sağlayıcı yönetim politikasına uygun olarak hizmet sağlayıcıları izleyin. İzleme, hizmet sağlayıcı uyumluluğunun periyodik olarak yeniden değerlendirilmesini, hizmet sağlayıcı sürüm notlarının izlenmesini ve karanlık web izlemesini içerebilir.			x	New				x				
15	15,7	Veri	Koruma (Protect)	Servis Sağlayıcıların Güvenli Bir Şekilde Hizmet Dışı Bırakılması	Servis sağlayıcıları güvenli bir şekilde devre dışı bırakın. Örnek hususlar arasında kullanıcı ve hizmet hesabının devre dışı bırakılması, veri akışlarının sonlandırılması ve kurumsal verilerin servis sağlayıcı sistemlerinde güvenli bir şekilde elden çıkarılması sayılabilir.			x	New				x				
16	16,3	Uygulamalar	Koruma (Protect)	Güvenlik Açıkları Üzerinde Kök Neden Analizi Gerçekleştirme	Güvenlik açıkları üzerinde kök neden analizi yapın. Güvenlik açıklarını gözden geçirirken, kök neden analizi, kodda güvenlik açıkları oluşturan temel sorunları değerlendirme görevidir ve geliştirme ekiplerinin ortaya çıktıkça yalnızca bireysel güvenlik açıklarını düzeltmenin ötesine geçmesine izin verir.		x	x	New				x				
16	16,4	Uygulamalar	Koruma (Protect)	Üçüncü Taraf Yazılım Bileşenleri Envanterini Oluşturun ve Yönetin	Geliştirmede kullanılan ve genellikle "malzeme listesi" olarak adlandırılan üçüncü taraf bileşenlerinin ve ayrıca gelecekte kullanılmak üzere planlanan bileşenlerin güncellenmiş bir envanterini oluşturun ve yönetin. Bu envanter, her bir üçüncü taraf bileşeninin oluşturabileceği riskleri içerecektir. Bu bileşenlerde yapılan değişiklikleri veya güncellemeleri belirlemek için listeyi en az ayda bir değerlendirin ve bileşenin hala desteklendiğini doğrulayın.		x	x	New				x				
16	16,6	Uygulamalar	Koruma (Protect)	Uygulama Güvenlik Açıkları için Önem Derecelendirme Sistemi ve Süreci Oluşturun ve Sürdürün	Keşfedilen güvenlik açıklarının düzeltildiği sıraya öncelik verilmesini kolaylaştıran uygulama güvenlik açıkları için bir önem derecesi derecelendirme sistemi ve süreci oluşturun ve sürdürün. Bu süreç, kod veya uygulamaları serbest bırakmak için minimum güvenlik kabul edilebilirliği düzeyini ayarlamayı içerir. Önem dereceleri, risk yönetimini geliştiren ve en ciddi hataların ilk önce düzeltilmesini sağlamaya yardımcı olan güvenlik açıklarını tetiklemek için sistematik bir yol sunar. Sistemi ve süreci yıllık olarak gözden geçirin ve güncelleyin.		x	x	New				x				
16	16,10	Uygulamalar	Koruma (Protect)	Uygulama Mimarilerinde Güvenli Tasarım İlkelerini Uygulayın	Uygulama mimarilerinde güvenli tasarım ilkelerini uygulayın. Güvenli tasarım ilkeleri, en az ayrıcalık kavramını ve kullanıcının yaptığı her işlemi doğrulamak için arabuluculuğu zorunlu kılarak "kullanıcı girdisine asla güvenme" kavramını teşvik eder. Örnekler, boyut, veri türü ve kabul edilebilir aralıklar veya biçimler dahil olmak üzere tüm girdiler için açık hata denetiminin gerçekleştirilmesini ve belgelenmesini içerir. Güvenli tasarım ayrıca, korumasız bağlantı noktalarını ve hizmetleri kapatmak, gereksiz programları ve dosyaları kaldırmak ve varsayılan hesapları yeniden adlandırmak veya kaldırmak gibi uygulama altyapısı saldırı yüzeyini en aza indirmek anlamına gelir.		x	x	New				x				
16	16,11	Uygulamalar	Koruma (Protect)	Uygulama Güvenliği Bileşenleri için Kontrol Edilen Modüller veya Hizmetlerden Yararlanın	Kimlik yönetimi, şifreleme ve denetleme ve günlüğe kaydetme gibi uygulama güvenliği bileşenleri için onaylanmış modüllerden veya hizmetlerden yararlanın. Platform özelliklerinin kritik güvenlik işlevlerinde kullanılması, geliştiricilerin iş yükünü azaltacak ve tasarım veya uygulama hataları olasılığını en aza indirecektir. Modern işletim sistemleri, tanımlama, kimlik doğrulama ve yetkilendirme için etkili mekanizmalar sağlar ve bu mekanizmaları uygulamalar için kullanılabilir hale getirir. Yalnızca standartlaştırılmış, şu anda kabul edilmiş ve kapsamlı bir şekilde gözden geçirilmiş şifreleme algoritmalarını kullanın. İşletim sistemleri ayrıca güvenli denetim günlükleri oluşturmak ve sürdürmek için mekanizmalar sağlar.		x	x	New				x				
16	16,12	Uygulamalar	Koruma (Protect)	Kod Düzeyinde Güvenlik Kontrolleri Uygulayın	Güvenli kodlama uygulamalarının takip edildiğini doğrulamak için uygulama yaşam döngüsü içinde statik ve dinamik analiz araçları uygulayın.			x	New				x				
16	16,13	Uygulamalar	Koruma (Protect)	Uygulama Sızma Testini Gerçekleştirin	Uygulama penetrasyon testi yapın. Kritik uygulamalar için, kimliği doğrulanmış sızma testi, iş mantığı güvenlik açıklarını bulmak için kod tarama ve otomatik güvenlik testinden daha uygundur. Penetrasyon testi, test cihazının bir uygulamayı kimliği doğrulanmış ve kimliği doğrulanmamış bir kullanıcı olarak manuel olarak değiştirme becerisine dayanır.			x	New				x				
16	16,14	Uygulamalar	Koruma (Protect)	Tehdit Modelleme Yapın	Tehdit modellemesi yapın. Tehdit modelleme, kod oluşturulmadan önce bir tasarımdaki uygulama güvenliği tasarım kusurlarını belirleme ve ele alma sürecidir. Uygulama tasarımını değerlendiren ve her giriş noktası ve erişim seviyesi için güvenlik risklerini ölçen özel eğitimli kişiler tarafından gerçekleştirilir. Amaç, zayıflıklarını anlamak için uygulamayı, mimariyi ve altyapıyı yapılandırılmış bir şekilde haritalandırmaktır.			x	New				x				
17	17,6	N/A	Cevapla (Respond)	Olay Müdahalesi Sırasında İletişim İçin Mekanizmaları Tanımlayın	Bir güvenlik olayı sırasında iletişim kurmak ve raporlamak için hangi birincil ve ikincil mekanizmaların kullanılacağını belirleyin. Mekanizmalar telefon görüşmelerini, e-postaları veya mektupları içerebilir. Bir güvenlik olayı sırasında e-postalar gibi belirli mekanizmaların etkilenebileceğini unutmayın. Yıllık olarak veya bu Korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin.		x	x	New				x				
17	17,8	N/A	Kurtarma (Recover)	Olay Sonrası İncelemeleri Yürütün	Olay sonrası incelemeler yapın. Olay sonrası incelemeler, öğrenilen dersleri ve takip eylemini belirleyerek olayın tekrarını önlemeye yardımcı olur.		x	x	New				x				
18	18,3	Ağ	Koruma (Protect)	Penetrasyon Testi Bulgularını Düzeltin	Kuruluşun iyileştirme kapsamı ve önceliklendirme politikasına dayalı olarak sızma testi bulgularını düzeltin.		x	x	New				x				
18	18,4	Ağ	Koruma (Protect)	Güvenlik Önlemlerini Doğrulayın	Her sızma testinden sonra güvenlik önlemlerini doğrulayın. Gerekirse, test sırasında kullanılan teknikleri tespit etmek için kural kümelerini ve yetenekleri değiştirin.			x	New				x				
1	**1**			**Kurumsal Varlıkların Envanteri ve Kontrolü**	***Altyapıya fiziksel, sanal olarak bağlı tüm kurumsal varlıkları (taşınabilir ve mobil dahil son kullanıcı cihazları; ağ cihazları; bilgi işlem dışı/Nesnelerin İnterneti (IoT) cihazları ve sunucular) aktif olarak yönetin (envanterini çıkarın, izleyin ve düzeltin), kurum içinde izlenmesi ve korunması gereken varlıkların toplamını doğru bir şekilde bilmek için uzaktan ve bulut ortamlarındakiler. Bu ayrıca, kaldırılacak veya düzeltilecek yetkisiz ve yönetilmeyen varlıkların belirlenmesini de destekleyecektir.***												
2	**2**			**Yazılım Varlıklarının Envanteri ve Kontrolü**	***Ağdaki tüm yazılımları (işletim sistemleri ve uygulamaları) etkin bir şekilde yönetin (envanterini çıkarın, izleyin ve düzeltin), böylece yalnızca yetkilendirilmiş yazılımlar kurulur ve yürütülür, yetkisiz ve yönetilmeyen yazılımlar bulunur ve kurulum veya yürütmenin önlenmesi sağlanır.***												
3	**3**			**Veri koruması**	***Verileri belirlemek, sınıflandırmak, güvenli bir şekilde işlemek, saklamak ve elden çıkarmak için süreçler ve teknik kontroller geliştirin.***												
4	**4**			**Kurumsal Varlıkların ve Yazılımın Güvenli Yapılandırması**	***Kurumsal varlıkların (taşınabilir ve mobil dahil son kullanıcı cihazları; ağ cihazları; bilgi işlem dışı/IoT cihazları ve sunucular) ve yazılımların (işletim sistemleri ve uygulamaları) güvenli yapılandırmasını oluşturun ve sürdürün.***												
5	**5**			**Hesap Yönetimi**	***Yönetici hesaplarının yanı sıra hizmet hesapları da dahil olmak üzere kullanıcı hesaplarına, kurumsal varlıklara ve yazılımlara yönelik kimlik bilgilerine yetki atamak ve yönetmek için süreçleri ve araçları kullanın.***												
6	**6**			**Erişim Kontrol Yönetimi**	***Kurumsal varlıklar ve yazılımlar için kullanıcı, yönetici ve hizmet hesapları için erişim kimlik bilgileri ve ayrıcalıkları oluşturmak, atamak, yönetmek ve iptal etmek için süreçleri ve araçları kullanın.***												
7	**7**			**Sürekli Güvenlik Açığı Yönetimi**	***Saldırganlar için fırsat penceresini düzeltmek ve en aza indirmek için kuruluşun altyapısındaki tüm kurumsal varlıklardaki güvenlik açıklarını sürekli olarak değerlendirmek ve izlemek için bir plan geliştirin. Yeni tehdit ve güvenlik açığı bilgileri için kamu ve özel sektör kaynaklarını izleyin.***												
8	**8**			**Denetim Günlüğü Yönetimi**	***Bir saldırıyı tespit etmeye, anlamaya veya saldırıdan kurtarmaya yardımcı olabilecek olayların denetim günlüklerini toplayın, uyarın, inceleyin ve saklayın.***												
9	**9**			**E-posta ve Web Tarayıcı Korumaları**	***Saldırganların doğrudan etkileşim yoluyla insan davranışlarını manipüle etme fırsatları olduğundan, e-posta ve web vektörlerinden gelen tehditlerin korumasını ve algılamasını iyileştirin.***												
10	**10**			**Kötü Amaçlı Yazılım Savunmaları**	***Kurumsal varlıklar üzerinde kötü amaçlı uygulamaların, kodların veya komut dosyalarının yüklenmesini, yayılmasını ve yürütülmesini önleyin veya kontrol edin.***												
11	**11**			**Veri kurtarma**	***Kapsam dahilindeki kurumsal varlıkları olay öncesi ve güvenilir bir duruma geri yüklemek için yeterli veri kurtarma uygulamalarını oluşturun ve sürdürün.***												

12	12			Ağ Altyapısı Yönetimi	*Saldırganların savunmasız ağ hizmetlerinden ve erişim noktalarından yararlanmasını önlemek için ağ cihazlarını kurun, uygulayın ve aktif olarak yönetin (izleyin, raporlayın, düzeltin).*												
13	13			Ağ İzleme ve Savunma	*Kuruluşun ağ altyapısı ve kullanıcı tabanı genelinde kapsamlı ağ izleme ve güvenlik tehditlerine karşı savunma oluşturmak ve sürdürmek için süreçleri ve araçları çalıştırın.*												
14	14			Güvenlik Bilinci ve Becerileri Eğitimi	*Kuruma yönelik siber güvenlik risklerini azaltmak için güvenlik bilincine sahip ve uygun becerilere sahip olmak için işgücü arasındaki davranışları etkilemek için bir güvenlik bilinci programı oluşturun ve sürdürün.*												
15	15			Servis Sağlayıcı Yönetimi	*Hassas verileri elinde bulunduran veya bir kuruluşun kritik BT platformlarından veya süreçlerinden sorumlu olan hizmet sağlayıcıların bu platformları ve verileri uygun şekilde koruduğundan emin olmak için bir süreç geliştirin.*												
16	16			Uygulama Yazılım Güvenliği	*Güvenlik zayıflıklarını işletmeyi etkilemeden önce önlemek, tespit etmek ve gidermek için kurum içinde geliştirilen, barındırılan veya satın alınan yazılımların güvenlik yaşam döngüsünü yönetin.*												
17	17			Olay Müdahale Yönetimi	*Bir saldırıyı hazırlamak, tespit etmek ve hızlı bir şekilde yanıt vermek için bir olay müdahale yeteneği (ör. politikalar, planlar, prosedürler, tanımlanmış roller, eğitim ve iletişimler) geliştirmek ve sürdürmek için bir program oluşturun.*												
18	18			Penetrasyon testi	*Denetimlerdeki (insanlar, süreçler ve teknoloji) zayıflıkları belirleyip bunlardan yararlanarak ve bir saldırganın amaçlarını ve eylemlerini simüle ederek kurumsal varlıkların etkinliğini ve esnekliğini test edin.*												