0’dan 82’ye Siber Güvenlik

82 Adımdan Oluşan Siber Güvenlik Rehberi ile Şirketinizin Güvenlik Altyapısını Güçlendirin

Bu rehber, siber tehditlere karşı dayanıklılığınızı artırmak amacıyla adım adım uygulamanız gereken çözümlerin listesini sunar.

PitGrowth, teknoloji şirketleri, kurumsal firmalar, yatırımcılar, teknoloji merkezleri ve ekosistem paydaşlarını tek bir platformda buluşturan global bir listeleme ve B2B eşleştirme platformudur.

PitGrowth tarafından hazırlanan rehberde platformda yer alan 1000’den fazla Türk siber güvenlik şirketi incelenmiştir. Siber güvenlik odağındaki bu şirketlerin yalnızca 120’si siber güvenlik odaklı ürün / ürünler geliştirmiştir. Bu şirketlerden 90’ı ile bire bir görüşmeler gerçekleştirilmiş olup, kategoriler ve içerikler, alanında uzman siber güvenlik profesyonellerinin desteği ile oluşturulmuştur.

Amacımız, Türkiye'deki siber güvenlik ekosisteminde faaliyet gösteren şirketlerin sunduğu hizmetleri ve ürünlerin kullanım alanlarını analiz ederek, şirketler için kapsamlı bir yol haritası sunmayı hedefliyoruz.

Kontrol Listesi İçeriğinde mikro işletmeler, KOBİ'ler ve kurumsal şirketler için hazırlanan kontrol listesinde şunları bulacaksınız

- Ana Siber Güvenlik Kategorileri
- Alt Siber Güvenlik Kategorileri
- Siber Güvenlik Çözümlerin Tanımı
- Şirketiniz İçin Kontrol Soruları
- Riskler
- Çözümü Şirketinizde Neden Kullanmanız Gerekiyor?
- Sonraki Adımda Neler Yapılmalı?
- Çözümleri Hangi Tür İşletmeler Kullanmalı?*
- Çözümleri Hangi Endüstriler Kullanmalı?*
- Çözümler Kaç Çalışanlı Şirketler İçin Uygun?*
- Çözümler Şirketler İçin Temel Gereklilik mi?*
- Türkiye’de Hangi Kategorilerde Hangi Şirketlerin Ürünleri Var?*

İçindekiler

360° Siber Güvenlik 2
Rakamlarla Siber Güvenlik 3
Siber Güvenlik Ana Kategorileri ..... 4 - 6
Şirketler için Kontrol Listesi ..... 7 - 17
Detaylar 18

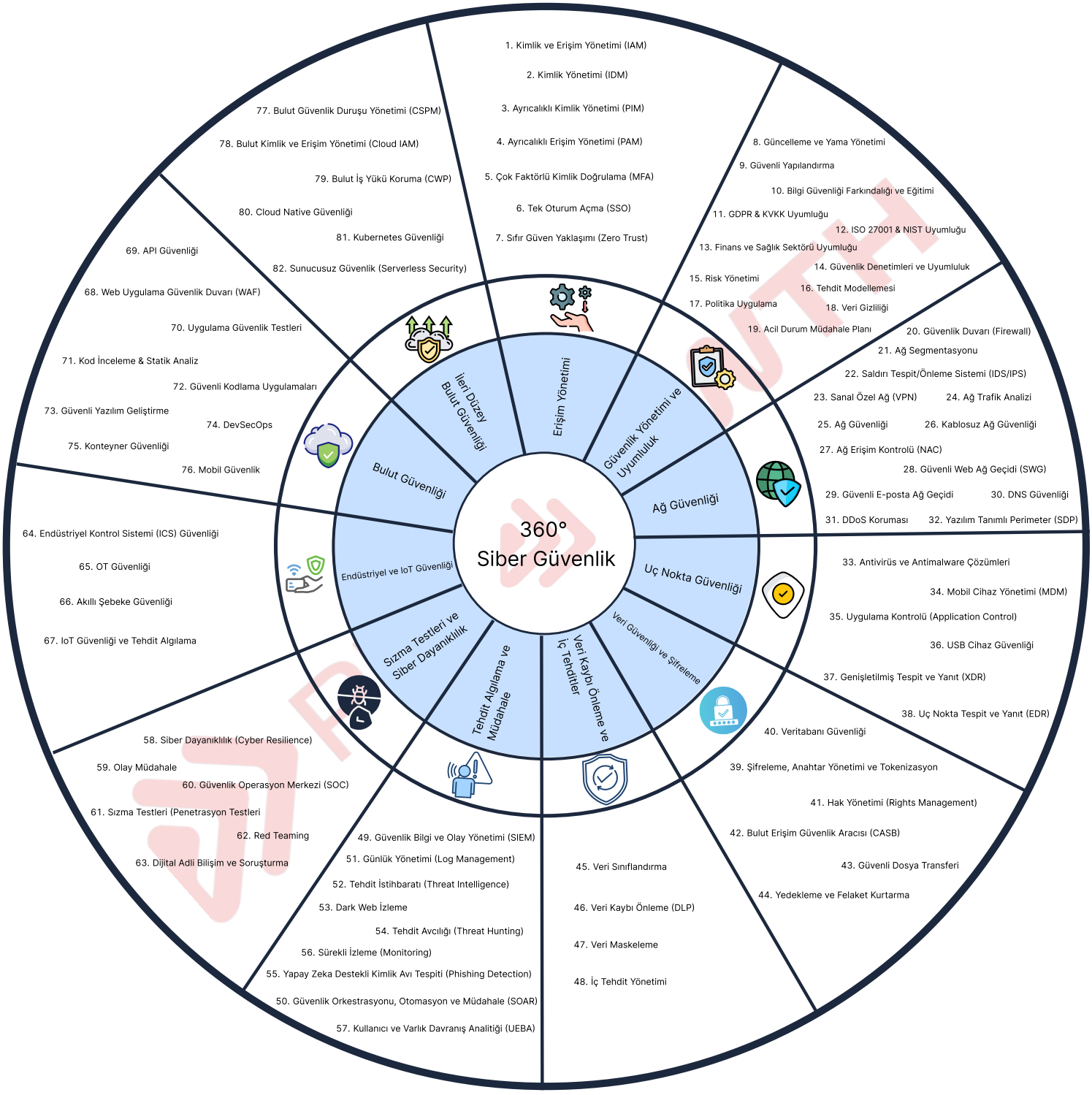
⚠️ **Başlamadan Önce Okuyunuz :**

- Bu rapor sadece bilgilendirme amaçlıdır.
- Şirketinizin büyüklüğüne ve faaliyet alanına göre ihtiyaç sıralaması değişiklik gösterebilir.
- Kontrol listesindeki bazı çözümler, belirli şirketler için gerekli olmayabilir.
- Şirketinizin siber güvenlik planlaması ve uygulanması için mutlaka bir uzmandan destek almanızı öneririz.
- Kontrol listesindeki sıralama siber güvenlik profesyonellerinden aldığımız yönlendirmelere göre tasarlanmıştır. Şirketlerin önceliklerine göre değişkenlik gösterebilir.
- İşaretli * detaylar için kurumsal üyelik gereklidir.

Saygılarımızla,

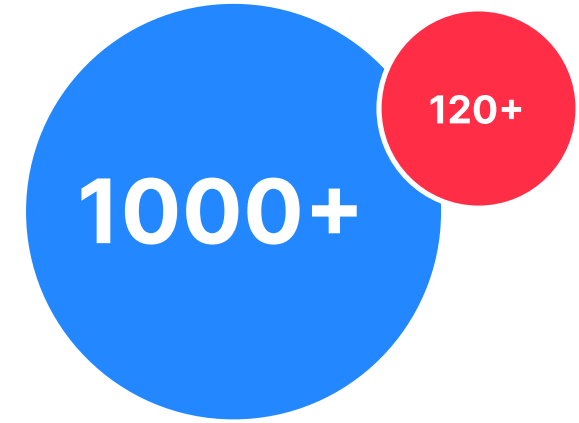
Pit Team

360° Siber Güvenlik

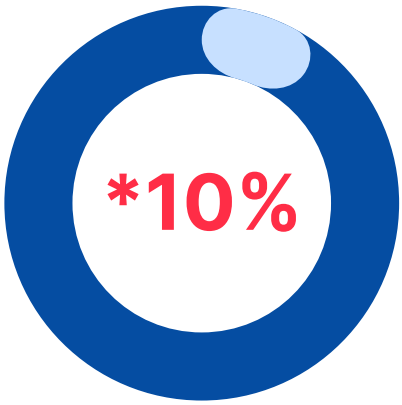


Rakamlarla Siber Güvenlik

Siber güvenlik odaklı Türk teknoloji şirketlerinin sayısı



Yatırım Alan Siber Güvenlik Şirketlerin Oranı



Siber Güvenlik Ana Kategorileri	Ürün ve Şirket Sayısı*
Erişim Yönetimi	23
Güvenlik Yönetimi ve Uyumluluk	19
Ağ Güvenliği	23
Uç Nokta Güvenliği	21
Veri Güvenliği ve Şifreleme	20
Veri Kaybı Önleme ve İç Tehditler	15
Tehdit Algılama ve Müdahale	25
Sızma Testleri ve Siber Dayanıklılık	12
Endüstriyel ve IoT Güvenliği	5
Bulut Güvenliği	25
İleri Düzey Bulut Güvenliği	8

* Ana kategorilerde siber güvenlik ürünü bulunan şirketlerin sayılarını göstermektedir. Bu veriler, bire bir görüşülen şirketler dışında, siber güvenlik odaklı ürün geliştiren şirketlerin web sayfaları baz alınarak oluşturulmuştur.

* Yatırım alan siber güvenlik şirketleri, tüm siber güvenlik şirketleri (hizmet sağlayıcı, danışman şirketler, ürün geliştiren şirket...vb) de dahil halka açık yatırım sayıları baz alınarak gösterilmiştir. Sadece kendi siber ürününü geliştiren şirketler baz alındığında yatırım alan siber güvenlik şirket sayısı yaklaşık olarak %60'tır.

Siber Güvenlik Ana Kategorileri

1.0 Erişim Yönetimi 7
1.1 Kimlik ve Erişim Yönetimi (IAM)
1.2 Kimlik Yönetimi (IDM)
1.3 Ayrıcalıklı Kimlik Yönetimi (PIM)
1.4 Ayrıcalıklı Erişim Yönetimi (PAM)
1.5 Çok Faktörlü Kimlik Doğrulama (MFA)
1.6 Tek Oturum Açma (SSO)
1.7 Sıfır Güven Yaklaşımı (Zero Trust)

2.0 Güvenlik Yönetimi ve Uyumluluk 8
2.1 Güncelleme ve Yama Yönetimi
2.2 Güvenli Yapılandırma
2.3 Bilgi Güvenliği Farkındalığı ve Eğitimi
2.4 GDPR & KVKK Uyumluğu
2.5 ISO 27001 & NIST Uyumluğu
2.6 Finans ve Sağlık Sektörü Uyumluğu
2.7 Güvenlik Denetimleri ve Uyumluluk
2.8 Risk Yönetimi
2.9 Tehdit Modellemesi
2.10 Politika Uygulama
2.11 Veri Gizliliği
2.12 Acil Durum Müdahale Planı

3.0 Ağ Güvenliği 9
3.1 Güvenlik Duvarı (Firewall)
3.2 Ağ Segmentasyonu
3.3 Saldırı Tespit/Önleme Sistemi (IDS/IPS)
3.4 Sanal Özel Ağ (VPN)
3.5 Ağ Trafik Analizi
3.6 Ağ Güvenliği
3.7 Kablosuz Ağ Güvenliği
3.8 Ağ Erişim Kontrolü (NAC)
3.9 Güvenli Web Ağ Geçidi (SWG)
3.10 Güvenli E-posta Ağ Geçidi
3.11 DNS Güvenliği
3.12 DDoS Koruması
3.13 Yazılım Tanımlı Perimeter (SDP)

Siber Güvenlik Ana Kategorileri

4.0 Uç Nokta Güvenliği 10
4.1 Antivirüs ve Antimalware Çözümleri
4.2 Mobil Cihaz Yönetimi (MDM)
4.3 Uygulama Kontrolü (Application Control)
4.4 USB Cihaz Güvenliği
4.5 Genişletilmiş Tespit ve Yanıt (XDR)
4.6 Uç Nokta Tespit ve Yanıt (EDR)

5.0 Veri Güvenliği ve Şifreleme 11
5.1 Veritabanı Güvenliği
5.2 Şifreleme, Anahtar Yönetimi ve Tokenizasyon
5.3 Hak Yönetimi (Rights Management)
5.4 Bulut Erişim Güvenlik Aracısı (CASB)
5.5 Güvenli Dosya Transferi
5.6 Yedekleme ve Felaket Kurtarma

6.0 Veri Kaybı Önleme ve İç Tehditler 12
6.1 Veri Sınıflandırma
6.2 Veri Kaybı Önleme (DLP)
6.3 Veri Maskeleme
6.4 İç Tehdit Yönetimi

7.0 Tehdit Algılama ve Müdahale 13
7.1 Güvenlik Bilgi ve Olay Yönetimi (SIEM)
7.2 Güvenlik Orkestrasyonu, Otomasyon ve Müdahale (SOAR)
7.3 Günlük Yönetimi (Log Management)
7.4 Tehdit İstihbaratı (Threat Intelligence)
7.5 Dark Web İzleme
7.6 Tehdit Avcılığı (Threat Hunting)
7.7 Yapay Zeka Destekli Kimlik Avı Tespiti (Phishing Detection)
7.8 Sürekli İzleme (Monitoring)
7.9 Kullanıcı ve Varlık Davranış Analitiği (UEBA)

Siber Güvenlik Ana Kategorileri

8.0 Sızma Testleri ve Siber Dayanıklılık 14
8.1 Siber Dayanıklılık (Cyber Resilience)
8.2 Olay Müdahale
8.3 Güvenlik Operasyon Merkezi (SOC)
8.4 Sızma Testleri (Penetrasyon Testleri)
8.5 Red Teaming
8.6 Dijital Adli Bilişim ve Soruşturma

9.0 Endüstriyel ve IoT Güvenliği 15
9.1 Endüstriyel Kontrol Sistemi (ICS) Güvenliği
9.2 OT Güvenliği
9.3 Akıllı Şebeke Güvenliği
9.4 IoT Güvenliği ve Tehdit Algılama

10.0 Bulut Güvenliği 16
10.1 Web Uygulama Güvenlik Duvarı (WAF)
10.2 API Güvenliği
10.3 Uygulama Güvenlik Testleri
10.4 Kod İnceleme & Statik Analiz
10.5 Güvenli Kodlama Uygulamaları
10.6 Güvenli Yazılım Geliştirme
10.7 DevSecOps
10.8 Konteyner Güvenliği
10.9 Mobil Güvenlik

11.0 İleri Düzey Bulut Güvenliği 17
11.1 Bulut Güvenlik Duruşu Yönetimi (CSPM)
11.2 Bulut Kimlik ve Erişim Yönetimi (Cloud IAM)
11.3 Bulut İş Yükü Koruma (CWP)
11.4 Cloud Native Güvenliği
11.5 Kubernetes Güvenliği
11.6 Sunucusuz Güvenlik (Serverless Security)

1.0 Erişim Yönetimi

	1.0 Erişim Yönetimi	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	1.1 Kimlik ve Erişim Yönetimi (IAM)	Kullanıcıların dijital kimliklerini doğrulayan ve erişim haklarını yöneten sistemlerdir. Kurumların "kim, neye, ne zaman erişebilir?" sorusuna yanıt verir.	Yeni bir çalışanın sisteme erişimi 1 günden uzun sürüyor mu?	Büyük şirketlerde manuel erişim yönetimi hatalara ve güvenlik açıklarına yol açar. Örneğin, pazarlama ekibindeki bir çalışan yanlışlıkla müşteri kredi kartı verilerine erişebilir. IAM, bu süreci otomatize ederek RBAC (Rol Tabanlı Erişim Kontrolü) gibi modellerle yetkileri dinamik olarak yönetir. Yetersiz erişim kontrolü, yanlış departmanlara gereksiz sistem erişimi sağlayabilir ve ciddi güvenlik riskleri oluşturabilir. Ancak, IAM'in sağlıklı çalışması için kimliklerin sistematik bir şekilde oluşturulup silinmesi kritiktir. Bu noktada, bir sonraki adım olarak Kimlik Yönetimi (IDM) sistemleri devreye girer.
	1.2 Kimlik Yönetimi (IDM)	Kurumdaki tüm kullanıcı hesaplarının yaşam döngüsünü yöneten sistemlerdir. Hesap oluşturma, güncelleme ve erişim iptali süreçlerini kapsar.	İşten ayrılan çalışanların hesapları 24 saat içinde kapatılıyor mu?	Her ay 50 yeni çalışan alan bir perakende şirketi, bu kişilere e-posta, ERP (Kurumsal Kaynak Planlama) ve CRM (Müşteri İlişkileri Yönetimi) hesaplarını otomatik oluşturabilir. İşten ayrılanların hesapları anında devre dışı bırakılarak "hayalet hesaplar" önlenir. Yetersiz hesap yönetimi, şirketin güvenlik açıklarını artırarak potansiyel veri sızıntısı riskini yükseltir. Ancak, tüm kimlikler eşit risk taşımaz. Özellikle yönetici hesapları gibi yüksek ayrıcalıklı kimlikler için standart IDM yetersiz kalır. Bu noktada bir sonraki adım olarak Ayrıcalıklı Kimlik Yönetimi (PIM) devreye girer.
	1.3 Ayrıcalıklı Kimlik Yönetimi (PIM)	Sistem yöneticileri, veritabanı adminleri veya CISO (Bilgi Güvenliği Baş Sorumlusu) gibi yüksek yetkili hesapların kimlik bilgilerinin güvenliğini sağlayan çözümlerdir.	Yönetici hesaplarının şifreleri her 90 günde bir değişiyor mu?	Bir e-ticaret şirketinde, tüm yöneticiler aynı "admin" şifresini kullanıyorsa, bu şifrenin sızması tüm sistemi çökertebilir. PIM, her yöneticiye özel kimlikler atayarak "paylaşılan şifre" riskini ortadan kaldırır. Yönetici erişimlerini "ihtiyaç anında" (just-in-time) vererek süreli yetkilendirme yapar. Fakat, bu hesapların kimliğini yönetmek yetmez; erişim anındaki davranışların izlenmesi de şarttır. Bu noktada bir sonraki adım olarak Ayrıcalıklı Erişim Yönetimi (PAM) zorunlu hale gelir.
	1.4 Ayrıcalıklı Erişim Yönetimi (PAM)	Yüksek yetkili hesapların kritik sistemlere yaptığı erişimlerin gerçek zamanlı izlenmesi, kayıt altına alınması ve şüpheli aktivitelerde anında müdahale edilmesini sağlayan sistemlerdir.	Yönetici işlemleri düzenli olarak denetleniyor mu?	Bir hastanede IT yöneticisi hasta veritabanına eriştiğinde, bu erişimin kaydedilmemesi durumunda yetki kötüye kullanımı tespit edilemez. PAM, tüm oturumları kaydederek "kim, ne yaptı?" sorusuna yanıt verir. Şüpheli bir komut çalıştırıldığında erişimi anında kesebilir. Ancak, erişim güvenliği için yalnızca izleme yeterli değildir. Kimlik doğrulama sürecinin güçlendirilmesi de kritiktir. Bu noktada bir sonraki adım olarak Çok Faktörlü Kimlik Doğrulama (MFA) devreye girer.
	1.5 Çok Faktörlü Kimlik Doğrulama (MFA)	Kullanıcıların kimliğini doğrulamak için birden fazla kanıt (şifre + SMS kodu + biyometri) isteyen güvenlik katmanıdır.	Finans veya IT ekipleri için MFA zorunlu mu?	Bir banka çalışanının şifresi phishing saldırısıyla çalınsa bile, MFA olmadan sisteme giriş yapılamaz. Bu, fidye yazılımlarını ve yetkisiz erişimleri %99,9 oranında engeller. Çoklu doğrulama adımları kullanıcı deneyimini zorlaştırabilir, bu yüzden kullanıcı dostu bir çözüm gereklidir. Bu dengeyi sağlamak için bir sonraki adım olarak Tek Oturum Açma (SSO) teknolojisi devreye girer.
	1.6 Tek Oturum Açma (SSO)	Kullanıcıların tek bir kimlik doğrulama işlemiyle (örneğin, Microsoft hesabı) birden fazla uygulamaya ve sisteme erişmesini sağlayan teknolojidir.	Şirket içi uygulamaların %90'ı tek bir girişle erişilebilir mi?	Çalışanların 10 farklı şifre hatırlaması, "şifre yorgunluğuna" ve zayıf şifre seçimine yol açar. SSO ile tüm uygulamalara tek bir güçlü şifreyle erişilir, bu da hem güvenliği hem verimliliği artırır. Ancak, SSO'nun güvenliği merkezi kimlik sağlayıcısının güvenilirliğine bağlıdır. Bu yüzden, tüm erişimlerde varsayılan güveni ortadan kaldıran bir yaklaşım gereklidir.
	1.7 Sıfır Güven Yaklaşımı (Zero Trust)	Hiçbir kullanıcıya, cihaza veya ağa varsayılan olarak güvenmeme" prensibine dayanan; her erişim isteğinin konum, cihaz durumu ve risk analizi gibi faktörlerle sürekli doğrulandığı bir güvenlik modelidir.	Erişim politikaları her kullanıcı ve cihaz için dinamik olarak mı belirleniyor?	Bir çalışan ofis ağındayken bile finans sistemine erişmek istediğinde, Zero Trust bu erişimi anında analiz eder. Çalışanın cihazı güncel olmayan bir yazılım kullanıyorsa veya erişim anormal bir saatteyse, ek doğrulama ister. Zero Trust, IAM, PAM ve SSO gibi tüm önceki adımları bir üst seviyeye taşıyarak, hibrit çalışma ve IoT (Nesnelerin İnterneti) gibi modern risklere karşı son savunma hattı oluşturur. Bu entegre yaklaşım, güvenlik yönetimi ve uyumluluk süreçlerimizin sürekli güncel ve etkili kalmasını sağlayarak, kurumsal savunma mekanizmalarımıza sağlam bir temel sunar.

2.0 Güvenlik Yönetimi ve Uyumluluk

	2.0 Güvenlik Yönetimi ve Uyumluluk	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	2.1 Güncelleme ve Yama Yönetimi	Güvenlik açıklarını en aza indirmek için sistemlerin, yazılımların ve donanımların düzenli olarak güncellenmesi ve yamalanması sürecidir.	Tüm sistemler kritik yamaları 48 saat içinde uyguluyor mu?"	Bir şirketin sunucularındaki eski yazılım sürümlerine sahip açıklar, siber saldırganlar için hedef olabilir. Özellikle fidye yazılımları ve sıfırıncı gün saldırıları, güncellenmemiş sistemleri hedef alarak büyük veri kayıplarına ve operasyonel aksaklıklara yol açabilir. Güncelleme ve yama yönetimi, sistemleri güncel tutarak bu zafiyetleri ortadan kaldırır ve sürekli tehdit izleme ile desteklenmelidir. Etkili bir güvenlik yönetimi için sadece yazılımların güncellenmesi yeterli değildir; aynı zamanda sistemlerin doğru yapılandırıldığından da emin olunmalıdır. Bu nedenle, güvenli yapılandırma, güvenlik yönetiminin bir diğer kritik bileşenidir.
	2.2 Güvenli Yapılandırma	Sistemlerin varsayılan ayarlarının güvenlik en iyi uygulamalarına uygun olarak optimize edilmesini sağlayan süreçtir.	Sistemlerde gereksiz servisler ve varsayılan hesaplar kaldırıldı mı?	Bir şirketin ağına bağlı sunucularda varsayılan şifreler ve kullanılmayan servisler, siber saldırılara açık kapı bırakabilir. Örneğin, yetkisiz erişimler ve kimlik avı saldırıları, güvenli yapılandırmanın eksik olduğu sistemlerde daha yaygındır. Güvenli yapılandırma, çok faktörlü kimlik doğrulama ve en az yetki prensibi gibi uygulamalarla desteklenmelidir. Ancak teknik önlemler tek başına yeterli değildir; çalışanların da bu konularda bilinçlendirilmesi gerekir. Bu nedenle, bilgi güvenliği farkındalığı ve eğitimi, güvenlik yönetiminin vazgeçilmez bir parçasıdır.
	2.3 Bilgi Güvenliği Farkındalığı ve Eğitimi	Çalışanların siber tehditler konusunda bilinçlendirilmesi ve güvenlik protokollerine uygun hareket etmeleri için eğitimler düzenlenmesini kapsar.	Çalışanlar her altı ayda bir siber güvenlik eğitimi alıyor mu?	Phishing saldırıları, çalışanların bilinçsiz hareketleri nedeniyle başarılı olabilir. Örneğin, sahte e-postalar ve sosyal mühendislik saldırıları, çalışanların farkında olmadan şirketin güvenliğini tehlikeye atmasına yol açabilir. Bilgi güvenliği eğitimleri, çalışanların farkındalığını artırarak siber riskleri minimize eder. Özellikle müşteri ve çalışan verilerinin korunması açısından, GDPR & KVKK uyumluluğu kritik bir gerekliliktir.
	2.4 GDPR & KVKK Uyumluluğu	Avrupa Birliği Genel Veri Koruma Tüzükü (GDPR) ve Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında, veri toplama, saklama ve paylaşım süreçlerinin uyumluluğu sağlanmalıdır.	Müşteri verileri için açık rıza alınıyor mu?	Bir şirket, GDPR veya KVKK uyumluluğunu sağlamazsa, yüksek miktarda cezalarla karşı karşıya kalabilir. Ayrıca, veri ihlalleri, şirketin itibarına zarar verebilir ve müşteri güvenini sarsabilir. Veri saklama süreçleri sürekli denetlenmeli ve güncellenmelidir. Veri güvenliğinin uluslararası standartlarla desteklenmesi için, ISO 27001 & NIST uyumluluğu büyük önem taşımaktadır.
	2.5 ISO 27001 & NIST Uyumluluğu	Bilgi güvenliği yönetim sistemleri için uluslararası standartlara uyum sağlamak amacıyla ISO 27001 ve NIST (National Institute of Standards and Technology) gereklilikleri uygulanmalıdır.	ISO 27001 sertifikasyon süreci tamamlandı mı?	ISO ve NIST standartları, kurumsal bilgi güvenliği altyapısını oluşturur ve güvenlik tehditlerine karşı şirketleri dayanıklı hale getirir. Uyumluluğun sağlanmaması durumunda, güvenlik açıkları ve mevzuat ihlalleri ciddi maliyetler doğurabilir. Özellikle finans ve sağlık sektörlerinde, güvenlik uyumluluğu daha da katı gereksinimler içermektedir.
	2.6 Finans ve Sağlık Sektörü Uyumluluğu	PCI-DSS (Payment Card Industry Data Security Standard) ve HIPAA (Health Insurance Portability and Accountability Act) gibi finans ve sağlık sektörü regülasyonlarına uyum sağlamak gerekir.	Tüm finansal işlemler şifreleniyor mu?"	Finansal verilerin çalınması veya hasta bilgilerinin sızması, büyük yasal ve maddi yaptırımlara neden olabilir. Örneğin, kredi kartı bilgileri veya hasta kayıtlarının sızdırılması, şirketlerin büyük tazminat davalarıyla karşılaşmasına sebep olabilir. Bu tür riskleri en aza indirmek için düzenli olarak güvenlik denetimleri ve uyumluluk süreçleri uygulanmalıdır.
	2.7 Güvenlik Denetimleri ve Uyumluluk	Şirketlerin güvenlik politikalarını ne kadar etkin uyguladığını belirlemek için düzenli iç ve dış denetimler gerçekleştirilmelidir.	Son güvenlik denetiminden sonra tespit edilen açıklar giderildi mi?	Denetimler olmadan güvenlik açıkları tespit edilemeyebilir ve bu durum saldırılara karşı savunmasızlık yaratır. Uyumluluk standartlarına uymayan şirketler, ciddi cezalarla karşılaşabilir. Güvenlik denetimlerinin ihmal edilmesi, hem veri ihlalleri hem de mevzuata aykırılıklar nedeniyle şirketlerin itibar ve finansal kayıplar yaşamasına sebep olabilir. Güvenlik tehditlerini öngörmek ve etkili stratejiler geliştirmek için risk yönetimi süreçleri uygulanmalıdır.
	2.8 Risk Yönetimi	Şirketlerin güvenlik tehditlerini tanımlaması, analiz etmesi ve etkilerini minimize etmesi için uygulanan süreçtir.	Risk değerlendirmeleri düzenli olarak yapılıyor mu?	Riskleri yönetmeden güvenlik politikaları tam anlamıyla başarılı olamaz. Siber tehditlerin sürekli evrim geçirdiği göz önüne alındığında, şirketler proaktif önlemler almalıdır. Risk yönetiminin ihmal edilmesi, beklenmedik güvenlik açıklarına ve operasyonel aksaklıklara yol açabilir. Ayrıca, finansal ve yasal riskleri artırarak şirketin uzun vadeli sürdürülebilirliğini tehdit edebilir. Riskleri etkin bir şekilde değerlendirmek ve sistemlerin savunmasını güçlendirmek için tehdit modellemesi süreçleri uygulanmalıdır.
	2.9 Tehdit Modellemesi	Olası saldırı vektörlerini belirleyerek, sistemlerin korunmasını sağlayan süreçtir.	Tüm kritik sistemler için tehdit modellemesi yapıldı mı?	Tehdit modellemesi, saldırı yüzeyini anlamaya ve güvenlik açıklarını önceden tespit etmeye yardımcı olur. Şirketler tehdit modellemesi yapmadığında, saldırganların sistemleri nasıl hedef alabileceğini öngöremeyerek savunmasız hale gelebilirler. Eksik tehdit modellemesi, hem maddi hem de operasyonel kayıplara sebep olabilir. Güvenlik stratejilerini etkili bir şekilde yürütmek için politika uygulama süreçlerinin eksiksiz olması gerekmektedir.
	2.10 Politika Uygulama	Bilgi güvenliği politikalarının oluşturulması, uygulanması ve denetlenmesi sürecidir.	Şirket içinde belirlenen güvenlik politikaları tüm çalışanlar tarafından uygulanıyor mu?	Güvenlik politikalarının oluşturulması ve etkin şekilde uygulanmaması, şirket içindeki güvenlik açıklarını artırır. Çalışanların politikaları tam olarak uygulamaması, veri ihlalleri ve uyumluluk problemlerine yol açabilir. Eksik veya yanlış uygulanan politikalar, saldırı risklerini artırarak şirketin güvenliğini zayıflatır. Veri güvenliğini daha üst seviyeye taşımak için veri gizliliği süreçleri titizlikle yönetilmelidir.
	2.11 Veri Gizliliği	Verilerin kim tarafından, nasıl işlendiğinin belirlenmesi ve korunması gereklidir.	Kritik verilerin kimler tarafından erişildiği takip ediliyor mu?	Veri gizliliği ihlal edildiğinde, şirketler hem yasal yaptırımlarla hem de müşteri güven kaybıyla karşılaşabilir. Kişisel veya hassas bilgilerin yetkisiz erişime maruz kalması, büyük maddi ve itibar kayıplarına yol açabilir. Güçlü veri gizliliği politikaları uygulanmadığında, hem mevzuat ihlalleri hem de siber saldırı riskleri artar. Veri güvenliğinin sürekli sağlanması, şirketin genel güvenlik yönetimi ve uyumluluk süreçlerinin ayrılmaz bir parçasıdır.
	2.12 Acil Durum Müdahale Planı	Olası güvenlik ihlalleri ve siber saldırılar karşısında alınacak aksiyonların önceden belirlenmesi gerekir.	Şirketin güncellenmiş bir acil durum müdahale planı var mı?	Acil durum planı olmadan, güvenlik ihlalleri ve saldırılar karşısında hızlı ve etkin bir müdahale yapılamaz. İyi planlanmış bir müdahale süreci, hasarı en aza indirir ve iş sürekliliğini sağlar. Acil durum müdahale planı olmayan şirketler, kriz anlarında büyük kayıplar yaşayabilir ve operasyonel aksaklıklarla karşılaşabilir.

3.0 Ağ Güvenliği

	3.0 Ağ Güvenliği	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	3.1 Güvenlik Duvarı (Firewall)	Güvenlik duvarı, iç ve dış ağlar arasındaki trafiği kontrol eden, belirli kurallar çerçevesinde erişim izni veren veya engelleyen donanım veya yazılım tabanlı çözümdür.	Ağ trafiği, güvenlik duvarı kurallarıyla düzenli olarak denetleniyor mu?	Güvenlik duvarı, potansiyel dış saldırıları engellemenin ilk savunma hattıdır. Yetkisiz erişimlerin önlenmesi, veri hırsızlığı ve kötü amaçlı yazılımların yayılmasının önüne geçilmesi için elzemdir. Güvenlik duvarı eksikliği, ağınızın savunmasız kalmasına ve ciddi veri ihlallerine neden olabilir. Bu nedenle, güvenli bir ağ yapısı oluşturmak amacıyla ağ segmentasyonu aşamasına geçilmesi gerekir.
	3.2 Ağ Segmentasyonu	Ağ segmentasyonu, büyük bir ağı, daha küçük ve izole alt bölümlere ayırarak her bölümün ayrı güvenlik politikaları ile korunmasını sağlayan yöntemdir.	Kritik veri bölgeleri izole edilip, ayrı güvenlik politikaları uygulanıyor mu?	Ağ segmentasyonu, bir bölgedeki güvenlik açığının tüm ağa sıçramasını engeller. Eksik segmentasyon, saldırganların tek bir noktadan tüm ağa yayılmasına zemin hazırlayabilir; bu da operasyonel aksaklıklar ve ciddi veri kayıpları riski yaratır. Bu nedenle, segmentasyon uygulaması son derece kritiktir ve bu koruma katmanının güçlendirilmesi için saldırı tespit/önleme sistemleri (IDS/IPS) kullanılmalıdır.
	3.3 Saldırı Tespit/Önleme Sistemi (IDS/IPS)	IDS/IPS sistemleri, ağ trafiğini sürekli izleyerek anormal aktiviteleri tespit eden ve bu aktiviteleri engelleyen çözümlerdir.	Ağda saldırı tespit ve önleme sistemleri etkin bir şekilde çalışıyor mu?	IDS/IPS, şüpheli aktiviteleri erkenden tespit ederek saldırıların yayılmasını engeller. Bu sistemlerin devre dışı bırakılması ya da yanlış yapılandırılması, ağda oluşabilecek tehditlerin gözden kaçmasına ve ciddi güvenlik açıklarının oluşmasına neden olabilir. Bu nedenle, IDS/IPS uygulamasının devamında, uzak bağlantıların güvenliğini sağlamak için sanal özel ağ (VPN) çözümlerine geçilmelidir.
	3.4 Sanal Özel Ağ (VPN)	VPN, internet üzerinden gerçekleşen veri iletişimini şifreleyerek güvenli bir tünel aracılığıyla gerçekleştirilmesini sağlayan teknolojidir.	Çalışanlar, uzak erişim için güvenli VPN bağlantıları kullanıyor mu?	VPN, verilerin şifrelenmiş şekilde iletilmesini sağlayarak, dış müdahalelere karşı koruma sunar. VPN kullanılmadığında, veriler açık olarak aktarılır; bu durum veri sızıntısı, kimlik hırsızlığı ve kötü niyetli erişim risklerini artırır. Bu nedenle, VPN uygulaması sonrası, ağ trafiğinin detaylı izlenmesi için ağ trafik analizi yapılmalıdır.
	3.5 Ağ Trafik Analizi	Ağ trafik analizi, ağdaki veri akışlarını sürekli izleyip analiz ederek anormallikleri ve potansiyel tehditleri tespit etmeye yarayan süreçtir.	Ağ trafiği düzenli olarak izleniyor ve şüpheli aktiviteler raporlanıyor mu?	Trafik analizi, olağan dışı hareketleri ve potansiyel saldırı girişimlerini erken aşamada belirler. İzleme yapılmadığında, saldırı girişimleri fark edilmeden devam edebilir; bu da geniş çaplı veri kayıplarına ve operasyonel aksaklıklara neden olabilir. Bu aşamadan sonra, özellikle mobil ve kablosuz erişim noktaları için kablosuz ağ güvenliği önem kazanır.
	3.6 Ağ Güvenliği	Ağ güvenliği, tüm ağ bileşenlerinin (cablolu ve kablosuz) bütünsel olarak korunması ve izlenmesini kapsar.	Şirketin ağ güvenliği için kapsamlı politikalar ve çözümler uygulanıyor mu?"	Ağ güvenliği, tüm ağ bileşenlerinde oluşabilecek tehditlere karşı koruma sağlar. Yetersiz uygulama, veri sızıntıları, sistem çöküşleri ve mali kayıplara neden olabilir. Bu nedenle, ağ güvenliğinin güçlendirilmesi sürecinde, özellikle kablosuz ağ güvenliği konusuna odaklanmak gerekir.
	3.7 Kablosuz Ağ Güvenliği	Kablosuz ağ güvenliği, Wi-Fi gibi kablosuz iletişim altyapılarının, yetkisiz erişim ve müdahalelere karşı korunmasını sağlar.	Kablosuz ağlar, güçlü şifreleme ve güncel güvenlik protokolleriyle korunuyor mu?	Kablosuz ağlar, sinyal yayılımı nedeniyle fiziksel sınırlar dışında da erişime açık olabilir. Zayıf kablosuz güvenlik, saldırganların ağa kolayca erişmesine ve veri çalınmasına yol açar. Bu risklerin önlenmesi, yetkisiz erişimlerin engellenmesi açısından kritiktir. Bu koruma katmanının ardından, ağdaki cihazların doğrulanması için ağ erişim kontrolü (NAC) uygulanmalıdır.
	3.8 Ağ Erişim Kontrolü (NAC)	NAC, ağa bağlanmak isteyen cihazların kimlik doğrulaması ve uyumluluk kontrollerini yaparak sadece yetkili cihazların erişimine izin veren bir güvenlik mekanizmasıdır.	Ağa bağlanan cihazlar, kimlik ve uyumluluk kontrollerinden geçiyor mu?"	NAC, kötü niyetli veya uyumsuz cihazların ağa erişimini engelleyerek veri güvenliğini artırır. Bu mekanizma olmadan, yetkisiz cihazların ağa dahil olması, veri ihlallerine ve sistem çöküşlerine yol açabilir. Bu riski minimize etmek için, kullanıcıların ve cihazların internet erişimini güvence altına almak amacıyla güvenli web ağ geçidi (SWG) uygulanmalıdır.
	3.9 Güvenli Web Ağ Geçidi (SWG)	SWG, kullanıcıların web trafiğini izleyerek zararlı içeriklere, kötü amaçlı sitelere ve phishing saldırılarına karşı filtreleme yapar.	Web trafiği, güvenli web ağ geçidi ile etkin bir şekilde filtreleniyor mu?	SWG, internete erişim sırasında ortaya çıkabilecek tehlikeleri önceden engelleyerek kullanıcıların verilerini korur. Filtreleme eksikliği, kötü amaçlı yazılımların ağa sızmasına ve veri ihlallerine neden olabilir. Bu riski azaltmak için, e-posta iletişiminin de güvenli hale getirilmesi gereklidir; bu amaçla güvenli e-posta ağ geçidi devreye alınmalıdır.
	3.10 Güvenli E-posta Ağ Geçidi	Güvenli e-posta ağ geçidi, e-posta trafiğini analiz ederek zararlı içerikleri, spam ve phishing saldırılarını engelleyen bir çözümdür.	E-posta trafiği, güvenli e-posta ağ geçidiyle zararlı içeriklere karşı korunuyor mu?	E-posta, siber saldırganlar için sıkça hedef alınan bir vektördür. Güvenli e-posta ağ geçidi, zararlı eklentiler ve phishing saldırılarının önüne geçerek veri güvenliğini artırır. Bu önlemin eksikliği, ciddi veri ihlallerine ve mali kayıplara yol açabilir. Bu koruma katmanının ardından, internet hizmetlerinin güvenliğini sağlamak için DNS güvenliği uygulanmalıdır.
	3.11 DNS Güvenliği	DNS güvenliği, domain isimlerinin doğru şekilde çözülmesini sağlayarak DNS tabanlı saldırılara karşı koruma sağlar.	DNS sorguları, güvenli yöntemlerle doğrulanıyor ve yönlendiriliyor mu?	DNS güvenliği, yanlış yönlendirme, DNS zehirlemesi gibi saldırıları engeller. DNS güvenliğinin ihmal edilmesi, kullanıcıların kötü niyetli sitelere yönlendirilmesine ve veri hırsızlığına zemin hazırlayabilir. Bu tehlikeleri azaltmak için, yüksek trafik saldırılarına karşı DDoS koruması devreye alınmalıdır.
	3.12 DDoS Koruması	DDoS koruması, ağınıza yönelik aşırı trafik saldırılarını tespit edip engelleyerek hizmet kesintilerini önleyen çözümler sunar.	Ağ, DDoS saldırılarına karşı etkili bir şekilde korunuyor mu?	DDoS saldırıları, ağ kaynaklarını aşırı yükleyerek hizmet dışı kalmasına neden olur. Bu saldırılar, mali kayıplara ve itibar zararına yol açabilir. DDoS korumasının eksikliği, kritik hizmetlerin kesintiye uğramasına neden olur. Bu riskin azaltılması için, son aşamada ileri düzey erişim kontrolü sağlayan yazılım tanımlı perimeter (SDP) teknolojisine geçilmelidir.
	3.13 Yazılım Tanımlı Perimeter (SDP)	SDP, her kullanıcı ve cihaz için dinamik olarak güvenlik sınırları belirleyerek ağ erişimini sıkı bir şekilde kontrol eden modern bir çözümdür.	Ağ erişimi, yazılım tanımlı perimeter teknolojisiyle güvence altına alınıyor mu?	SDP, ağdaki her cihazın ve kullanıcının kimlik doğrulamasını yaparak, izinsiz erişimleri önler. Bu teknoloji, eksik uygulandığında, saldırganların ağ içindeki hareket kabiliyetini artırabilir ve kritik verilerin çalınmasına neden olabilir. SDP ile ağ güvenliği, daha kapsamlı ve dinamik bir hale gelir; böylece tüm güvenlik önlemleri entegre bir sistem içinde korunur.

4.0 Uç Nokta Güvenliği

	4.0 Uç Nokta Güvenliği	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	4.1 Antivirüs ve Antimalware Çözümleri	Antivirüs ve antimalware çözümleri, bilgisayar sistemlerini virüsler, solucanlar, truva atları ve diğer kötü amaçlı yazılımlara karşı koruyan yazılımlardır.	Sistemlerimizde güncel ve etkin bir antivirüs ve antimalware çözümü kullanılıyor mu?	Kötü amaçlı yazılımlar, veri kaybına, sistem performansının düşmesine ve güvenlik ihlallerine yol açabilir. Antivirüs ve antimalware çözümleri, bu tür tehditleri tespit ederek sistemlerin güvenliğini sağlar. Bu çözümlerin kullanılmaması durumunda, sistemler kötü amaçlı yazılımlara karşı savunmasız hale gelir ve bu da veri ihlalleri, finansal kayıplar ve itibar zararına neden olabilir. Kötü amaçlı yazılımların mobil cihazlara da bulaşabileceği göz önüne alındığında, Mobil Cihaz Yönetimi (MDM) çözümleriyle tüm mobil cihazların güvenliği sağlanmalıdır.
	4.2 Mobil Cihaz Yönetimi (MDM)	MDM, işletmelerin mobil cihazlarını kaydetme, yapılandırma ve güvenliğini sağlama süreçlerini yöneten bir uygulamadır.	Şirketimizde kullanılan tüm mobil cihazlar MDM çözümleriyle yönetiliyor mu?	Mobil cihazlar, hassas kurumsal verilere erişim sağlayabilir. MDM çözümleri, bu cihazların güvenliğini ve uyumluluğunu sağlayarak veri sızıntılarını ve yetkisiz erişimleri önler. MDM kullanılmadığında, mobil cihazlar üzerinden veri sızıntısı, yetkisiz erişim ve kötü amaçlı yazılımların yayılması gibi riskler artar. Mobil cihazlardaki uygulamaların güvenliği de büyük önem taşır; bu nedenle, Uygulama Kontrolü ile yetkisiz veya riskli uygulamaların kullanımını engellemek gereklidir.
	4.3 Uygulama Kontrolü (Application Control)	Uygulama kontrolü, belirli yazılımların sistemlerde çalışmasına izin verme veya engelleme süreçlerini yöneten bir güvenlik önlemidir.	Sistemlerimizde yalnızca onaylanmış uygulamaların çalışmasına izin veriliyor mu?	Yetkisiz veya kötü amaçlı uygulamalar, sistem güvenliğini tehlikeye atabilir. Uygulama kontrolü, bu tür yazılımların çalıştırılmasını engelleyerek sistem bütünlüğünü korur. Uygulama kontrolü olmadan, kullanıcılar zararlı yazılımları çalıştırabilir, bu da veri ihlallerine ve sistem zararlarına yol açabilir. Taşınabilir depolama aygıtları da benzer riskler taşıdığından, USB Cihaz Güvenliği ile bu tür cihazların kullanımını denetlemek önemlidir.
	4.4 USB Cihaz Güvenliği	USB cihaz güvenliği, USB bellekler ve diğer taşınabilir depolama aygıtlarının kullanımını kontrol ederek, kötü amaçlı yazılımların ve yetkisiz veri transferlerinin önlenmesini amaçlayan bir güvenlik önlemidir.	USB cihazlarının kullanımı şirket politikalarına uygun şekilde denetleniyor mu?	USB cihazları, kötü amaçlı yazılımların yayılması ve hassas verilerin yetkisiz kişilerle paylaşılması için bir araç olabilir. Bu nedenle, USB cihazlarının kullanımını kontrol etmek, veri güvenliğini sağlamak açısından kritiktir. Denetimsiz USB kullanımı, veri sızıntılarına, kötü amaçlı yazılımların sisteme bulaşmasına ve ağ güvenliğinin tehlikeye girmesine neden olabilir. Gelişmiş tehditlerin tespiti ve yanıtı için, Genişletilmiş Tespit ve Yanıt (XDR) çözümleriyle sistem güvenliği daha da güçlendirilmelidir.
	4.5 Genişletilmiş Tespit ve Yanıt (XDR)	XDR, e-posta, uç nokta, sunucu, bulut iş yükü ve ağ gibi birden fazla güvenlik katmanından veri toplayarak, tehditleri daha hızlı tespit eden ve daha iyi araştırma ve müdahale süreleri sağlayan bir güvenlik çözümüdür.	XDR çözümleri, şirketimizin tüm güvenlik katmanlarında etkin bir şekilde uygulanıyor mu?	XDR, farklı güvenlik katmanlarından gelen verileri entegre ederek, tehditlerin daha hızlı ve kapsamlı bir şekilde tespit edilmesini ve müdahale edilmesini sağlar. Geleneksel güvenlik çözümleri, silo halinde çalıştığından, tehditlerin bütüncül bir perspektifle değerlendirilmesini engelleyebilir. XDR kullanılmadığında, tehditlerin tespiti gecikebilir ve bu da saldırıların etkisini artırabilir. Uç noktalarda daha spesifik tehdit tespiti ve yanıtı için, Uç Nokta Tespit ve Yanıt (EDR) çözümleriyle uç nokta güvenliği detaylı bir şekilde ele alınmalıdır.
	4.6 Uç Nokta Tespit ve Yanıt (EDR)	EDR, uç noktalarda gerçekleşen şüpheli etkinlikleri sürekli olarak izleyen, analiz eden ve bu tehditlere yanıt veren bir güvenlik çözümüdür.	EDR çözümleri, tüm uç nokta cihazlarımızda aktif olarak kullanılıyor mu?	EDR çözümleri, uç noktalarda gerçekleşen şüpheli etkinliklerin erken tespit edilmesini ve hızla müdahale edilmesini sağlayarak, veri ihlalleri ve operasyonel kesintilerin önüne geçer. Uç noktalarda EDR eksikliği, saldırıların fark edilmeden uzun süre devam etmesine ve ciddi mali zararların oluşmasına yol açabilir. Bu nedenle, uç nokta güvenliğini sağlamak için EDR kritik öneme sahiptir. EDR'nin etkin kullanımı, genel kurumsal güvenlik stratejimizin vazgeçilmez bir parçası olup, sonraki güvenlik katmanlarıyla entegre çalışarak kapsamlı bir savunma mekanizması oluşturur.

5.0 Veri Güvenliği ve Şifreleme

	5.0 Veri Güvenliği ve Şifreleme	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	5.1 Veritabanı Güvenliği	Veritabanı güvenliği, verilerin depolandığı sistemlerin yetkisiz erişim, veri kaybı veya değişiklik gibi tehditlere karşı korunmasını sağlar.	Sistemlerimizdeki veritabanları, güncel güvenlik önlemleriyle korunuyor mu?	Veritabanı güvenliği, kritik bilgilerin izinsiz erişim ve siber saldırılar sonucu çalınmasını veya bozulmasını engeller. Güvenlik açıklarının bulunması, hem finansal hem de itibari kayıplara yol açabilir. Bu nedenle, veritabanlarınızın korunması, veri bütünlüğü açısından elzemdir ve bunu takip eden koruyucu yöntemler, şifreleme gibi ek önlemlerle desteklenmelidir.
	5.2 Şifreleme, Anahtar Yönetimi ve Tokenizasyon	Şifreleme, verilerin okunamaz hale getirilmesi; anahtar yönetimi, şifreleme anahtarlarının güvenli şekilde saklanması; tokenizasyon ise hassas verilerin yerine sembolik değerlerin kullanılmasıdır.	Verilerimiz, güçlü şifreleme ve etkin anahtar yönetimi ile korunuyor mu?	Bu yöntemler, hassas bilgilerin çalınması veya değiştirilmesi riskini önemli ölçüde azaltır. Şifreleme uygulanmadığında, veriler ele geçirildiğinde doğrudan okunabilir ve zarar verebilir. Verilerin korunması sağlanırken, risklerin minimize edilmesi, veri güvenliğinin artırılmasını ve sonraki aşamada Hak Yönetimi gibi ek kontrollerin devreye alınmasını gerektirir.
	5.3 Hak Yönetimi (Rights Management)	Hak yönetimi, kullanıcılara ve gruplara erişim izinleri tanımlayarak, verilerin kimler tarafından görüntülenebileceğini veya düzenlenebileceğini kontrol eder.	Veri erişim izinleri, güncel ve doğru şekilde yönetiliyor mu?	Hak yönetimi, verilerin yalnızca yetkili kişiler tarafından erişilmesini sağlar ve yetkisiz erişim riskini düşürür. Yanlış yapılandırılmış izinler, veri sızıntılarına ve yetkisiz değişikliklere yol açabilir. Bu nedenle, doğru erişim kontrolleri sağlanmalı ve veri güvenliğinin bir sonraki aşaması olan Bulut Erişim Güvenlik Aracısı (CASB) çözümleri ile desteklenmelidir.
	5.4 Bulut Erişim Güvenlik Aracısı (CASB)	CASB, bulut hizmetlerine erişimi denetleyen ve verilerin bulut ortamında güvenli bir şekilde kullanılmasını sağlayan çözümler bütünüdür.	Bulut hizmetlerine erişim, CASB çözümleriyle kontrol ediliyor mu?	CASB, bulut ortamındaki veri transferleri ve uygulamalara yetkisiz erişimi engelleyerek veri güvenliğini artırır. Bu önlem alınmadığında, bulut tabanlı veri sızıntıları ve uyumsuzluklar ciddi riskler oluşturabilir. Bu nedenle, CASB kullanımı, verilerin güvenli bulut ortamında yönetilmesini sağlamak amacıyla, sonraki adım olarak Güvenli Dosya Transferi çözümlerine geçişi destekler.
	5.5 Güvenli Dosya Transferi	Güvenli dosya transferi, verilerin şifreleme ve diğer güvenlik protokolleri kullanılarak, güvenli bir şekilde iletilmesini sağlayan yöntemleri içerir.	Dosya transfer işlemleri, güvenli protokollerle gerçekleştiriliyor mu?	Güvenli dosya transferi, veri iletim sırasında oluşabilecek sızıntı ve müdahalelere karşı önemli bir koruma sağlar. Transfer sırasında verilerin ele geçirilmesi, hem mali kayıplara hem de itibari zararlar doğurabilir. Bu nedenle, dosya transferi güvenli bir şekilde yapılmalı ve bu korumanın devamı niteliğinde, veri kaybı ve felaket durumlarına karşı hazırlık için Yedekleme ve Felaket Kurtarma çözümleri devreye alınmalıdır.
	5.6 Yedekleme ve Felaket Kurtarma	Yedekleme ve felaket kurtarma, verilerin düzenli olarak yedeklenmesini ve olası bir veri kaybı durumunda hızlıca geri yüklenmesini sağlayan stratejilerdir.	Veriler düzenli olarak yedekleniyor ve felaket durumunda hızlıca kurtarılabiliyor mu?"	Yedekleme ve felaket kurtarma, veri kaybı, siber saldırılar veya donanım arızaları gibi durumlarda iş sürekliliğini sağlar. Yedeklerin eksik veya güncel olmaması, kritik verilerin kalıcı olarak kaybedilmesine yol açabilir. Bu nedenle, yedekleme stratejilerinin sağlam olması, veri bütünlüğünü korumak ve iş operasyonlarını sürdürebilmek için vazgeçilmezdir.

6.0 Veri Kaybı Önleme ve İç Tehditler

	6.0 Veri Kaybı Önleme ve İç Tehditler	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	6.1 Veri Sınıflandırma	Veri sınıflandırma, verileri önem ve duyarlılıklarına göre kategorilere ayırarak hangi koruma önlemlerinin uygulanacağını belirler.	Veriler, duyarlılık düzeylerine göre doğru şekilde sınıflandırılıyor mu?	Veri sınıflandırması, hangi verinin ne kadar korunması gerektiğini belirleyerek yanlışlıkla hassas bilgilerin açığa çıkmasını engeller. Sınıflandırma yapılmadığında, kritik veriler uygun güvenlik önlemleri olmadan işlenebilir ve riskler artar. Bu nedenle, veri sınıflandırması sağlanarak, sonraki adım olan veri kaybı önleme çözümlerine geçiş kolaylaştırılmalıdır.
	6.2 Veri Kaybı Önleme (DLP)	DLP çözümleri, hassas verilerin yetkisiz erişim, aktarım veya sızıntı riskini azaltmak için kullanılan teknolojilerdir.	Veri kaybı önleme sistemleri, hassas bilgilerin dışarı sızmasını etkili şekilde engelliyor mu?	DLP, veri sızıntılarını önleyerek mali kayıpları ve itibar zararını minimize eder; kullanılmadığında, veri hırsızlığı ve yanlışlıkla veri paylaşımı gibi ciddi riskler ortaya çıkar. Bu tür risklerin azaltılması için DLP çözümleri kritik öneme sahiptir. DLP uygulaması, veri maskeleme gibi ek tekniklerle desteklenerek kapsamlı bir veri koruma stratejisine geçişi sağlar.
	6.3 Veri Maskeleme	Veri maskeleme, hassas verilerin gerçek değerlerini gizleyerek, sadece yetkili kişilerin erişimine uygun hale getiren bir koruma yöntemidir.	Test ve geliştirme ortamlarında hassas veriler, etkili veri maskeleme teknikleriyle korunuyor mu?	Veri maskeleme, hassas bilgilerin yetkisiz erişimle ifşa olmasını engeller ve veri ihlallerinin etkisini azaltır; maskeleme uygulanmadığında, veriler yanlış ellere geçebilir ve ciddi zararlar meydana gelebilir. Bu riskin önüne geçmek için veri maskeleme, iç tehdit yönetimi stratejileriyle entegre edilmelidir. Böylece, hassas verilerin korunması sağlanarak güvenlik seviyesi artırılır.
	6.4 İç Tehdit Yönetimi	İç tehdit yönetimi, çalışanlar veya şirket içi aktörlerden kaynaklanabilecek veri ihlalleri ve kötü niyetli faaliyetleri tespit edip önlemeyi amaçlayan süreçleri kapsar.	İç tehditlere karşı proaktif izleme ve müdahale sistemleri kurulmuş mu?	İç tehditler, yetkisiz erişim veya kötü niyetli davranışlar sonucu veri güvenliğinde ciddi açıklar oluşturabilir; bu durum, dış saldırılardan daha yıkıcı sonuçlar doğurabilir. Yanlış yapılandırılmış erişim kontrolleri, veri sızıntılarına ve manipülasyona neden olabilir. Bu nedenle, iç tehdit yönetimi, veri sınıflandırması, DLP ve veri maskeleme ile entegre edilerek, kapsamlı ve bütünsel bir veri koruma stratejisi oluşturulmalıdır.

7.0 Tehdit Algılama ve Müdahale

	7.0 Tehdit Algılama ve Müdahale	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	7.1 Güvenlik Bilgi ve Olay Yönetimi (SIEM)	SIEM, farklı kaynaklardan gelen güvenlik verilerini toplayarak, gerçek zamanlı analiz ve tehdit tespiti sağlayan bir sistemdir.	SIEM sistemi, tüm güvenlik olaylarını merkezi olarak izleyip analiz ediyor mu?	SIEM, güvenlik olaylarını bütüncül bir bakış açısıyla değerlendirerek, anormal aktiviteleri hızla tespit eder ve müdahale sürecini hızlandırır; kullanılmadığında, tehditlerin fark edilmesi gecikebilir ve bu da ciddi güvenlik ihlallerine yol açabilir. SIEM'in etkin kullanımı, güvenlik süreçlerinin otomasyonu ve müdahale hızının artırılması için SOAR çözümleriyle entegre edilmelidir.
	7.2 Güvenlik Orkestrasyonu, Otomasyon ve Müdahale (SOAR)	SOAR, güvenlik operasyonlarını otomatikleştirerek, tehditlere karşı hızlı ve etkili müdahale sağlayan bir platformdur.	SOAR çözümleri, güvenlik süreçlerimizi ne kadar otomatikleştiriyor ve müdahale süremizi kısaltıyor mu?	SOAR, manuel müdahaleleri azaltarak güvenlik ekiplerinin verimliliğini artırır ve tehditlere karşı daha hızlı tepki verilmesini sağlar; kullanılmadığında, müdahale süreçleri yavaşlar ve bu da saldırıların etkisini artırabilir. SOAR'ın etkinliği, kapsamlı günlük yönetimi ile desteklenerek, tüm güvenlik verilerinin doğru ve zamanında işlenmesiyle artırılabilir.
	7.3 Günlük Yönetimi (Log Management)	Günlük yönetimi, sistem ve ağ cihazlarından gelen log verilerinin toplanması, depolanması ve analiz edilmesi sürecidir.	Tüm kritik sistemlerden gelen loglar düzenli olarak toplanıp analiz ediliyor mu?	Etkili bir günlük yönetimi, güvenlik olaylarının izlenmesi ve geçmişe dönük analizlerin yapılması için temel teşkil eder; logların yetersiz yönetimi, olayların tespitini ve analizini zorlaştırarak güvenlik açıklarına neden olabilir. Günlük yönetimi, tehdit istihbaratı ile entegre edilerek, potansiyel tehditlerin daha proaktif bir şekilde belirlenmesine katkı sağlar.
	7.4 Tehdit İstihbaratı (Threat Intelligence)	Tehdit istihbaratı, mevcut ve potansiyel tehditler hakkında bilgi toplayarak, güvenlik stratejilerini güçlendiren süreçtir.	Tehdit istihbaratı kaynaklarından gelen bilgiler düzenli olarak güvenlik politikalarımıza entegre ediliyor mu?	Tehdit istihbaratı, saldırıların önceden tahmin edilmesine ve savunma mekanizmalarının buna göre ayarlanmasına yardımcı olur; bu tür bilgiler olmadan, organizasyonlar yeni ve gelişen tehditlere karşı savunmasız kalabilir. Tehdit istihbaratı, dark web izleme faaliyetleriyle desteklenerek, siber suçluların faaliyetleri hakkında daha derinlemesine bilgi edinilmesini sağlar.
	7.5 Dark Web İzleme	Dark web izleme, organizasyonun hassas bilgilerinin karanlık ağda sızdırılıp sızdırılmadığını tespit etmek için yapılan sürekli bir takip sürecidir.	Şirketimize ait bilgiler dark web üzerinde düzenli olarak izleniyor ve sızıntılar tespit ediliyor mu?	Dark web izleme, hassas verilerin yetkisiz kişiler tarafından kullanılmasını engelleyerek, olası zararları minimize eder; bu tür bir izleme olmadan, veri sızıntıları geç fark edilebilir ve ciddi maddi ve manevi kayıplara yol açabilir. Dark web izleme, tehdit avcılığı süreçleriyle entegre edilerek, proaktif güvenlik önlemlerinin etkinliği artırılabilir.
	7.6 Tehdit Avcılığı (Threat Hunting)	Tehdit avcılığı, sistemlerde gizlenmiş ve geleneksel güvenlik önlemleriyle tespit edilemeyen tehditlerin proaktif olarak aranması sürecidir.	Sistemlerimizde düzenli olarak proaktif tehdit avcılığı yapılıyor mu?	Tehdit avcılığı, siber saldırganların izlerini erken aşamada tespit ederek, potansiyel zararları önler; bu süreç ihmal edildiğinde, saldırılar uzun süre fark edilmeden devam edebilir ve ciddi hasarlara neden olabilir. Tehdit avcılığı, yapay zeka destekli kimlik avı tespiti ile birleştiğinde, sosyal mühendislik saldırılarına karşı daha güçlü bir savunma sağlar.
	7.7 Yapay Zeka Destekli Kimlik Avı Tespiti (Phishing Detection)	Yapay zeka destekli kimlik avı tespiti, makine öğrenimi ve yapay zeka tekniklerini kullanarak, kimlik avı saldırılarını otomatik olarak tespit eden ve engelleyen bir süreçtir.	Yapay zeka tabanlı sistemlerimiz, kimlik avı girişimlerini etkin bir şekilde tespit edip engelliyor mu?	Geleneksel yöntemlerle tespiti zorlaşan gelişmiş kimlik avı saldırılarını belirlemek için yapay zeka tabanlı çözümler kritik öneme sahiptir; bu tür sistemlerin eksikliği, hassas bilgilerin çalınmasına ve ciddi güvenlik ihlallerine yol açabilir. Sürekli izleme mekanizmalarıyla birleştiğinde, güvenlik tehditlerine karşı daha kapsamlı bir koruma sağlanabilir.
	7.8 Sürekli İzleme (Monitoring)	Sürekli izleme, bilgi sistemlerinin ve ağların 7/24 takip edilerek, anormal aktivitelerin ve güvenlik olaylarının gerçek zamanlı olarak tespit edilmesi sürecidir.	Sistemlerimiz ve ağlarımız sürekli olarak izleniyor ve anormal aktiviteler anında tespit ediliyor mu?	Sürekli izleme, potansiyel tehditlerin erken aşamada belirlenmesini sağlayarak, olası zararları minimize eder; bu süreç ihmal edildiğinde, saldırılar uzun süre fark edilmeden devam edebilir ve ciddi hasarlara neden olabilir. Kullanıcı ve varlık davranış analitiği ile entegre edildiğinde, anormalliklerin tespiti daha da hassaslaşır ve güvenlik duruşu güçlenir.
	7.9 Kullanıcı ve Varlık Davranış Analitiği (UEBA)	UEBA, kullanıcıların ve varlıkların normal davranışlarını öğrenerek, bu davranışlardan sapmaları tespit eden ve olası güvenlik tehditlerini belirleyen bir güvenlik yaklaşımıdır.	UEBA çözümleri, kullanıcı ve varlık davranışlarındaki anormallikleri etkin bir şekilde tespit ediyor mu?	UEBA, içeriden gelen tehditleri ve gelişmiş saldırıları erken aşamada tespit ederek, proaktif güvenlik önlemleri alınmasını sağlar; bu tür bir analiz olmadan, anormal davranışlar gözden kaçabilir ve ciddi güvenlik ihlallerine yol açabilir. UEBA'nın etkin kullanımı, genel güvenlik stratejilerinin başarısını artırarak, organizasyonun siber tehditlere karşı direncini güçlendirir.

8.0 Sızma Testleri ve Siber Dayanıklılık

	8.0 Sızma Testleri ve Siber Dayanıklılık	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	8.1 Siber Dayanıklılık (Cyber Resilience)	Siber dayanıklılık, bir organizasyonun siber saldırılara karşı hazırlıklı olma, bu saldırılara etkin bir şekilde yanıt verme ve sonrasında hızla toparlanma yeteneğidir.	Şirketimiz, siber saldırılara karşı hazırlıklı mı ve olay sonrası hızlı bir şekilde toparlanabiliyor mu?"	Siber dayanıklılık, sürekli değişen tehdit ortamında iş sürekliliğini sağlamak için kritik öneme sahiptir; eksikliği, operasyonel aksaklıklara ve veri kayıplarına yol açabilir. Etkili bir siber dayanıklılık stratejisi, olay müdahale süreçlerinin etkinliğiyle doğrudan ilişkilidir.
	8.2 Olay Müdahale	Olay müdahale, siber güvenlik olaylarının tespiti, analizi ve etkilerinin minimize edilmesi için uygulanan süreçtir.	Şirketimizin siber güvenlik olaylarına karşı belirlenmiş bir müdahale planı var mı?	Hızlı ve etkili bir olay müdahale süreci, siber saldırıların zararlarını en aza indirir; bu süreçlerin eksikliği, veri ihlalleri ve finansal kayıplara neden olabilir. Olay müdahale süreçlerinin etkin yönetimi, Güvenlik Operasyon Merkezi'nin (SOC) varlığıyla desteklenir.
	8.3 Güvenlik Operasyon Merkezi (SOC)	SOC, organizasyonların bilgi sistemlerini 7/24 izleyen, analiz eden ve güvenlik olaylarına müdahale eden merkezi bir birimdir.	Şirketimizde güvenlik olaylarını sürekli izleyen ve yöneten bir SOC mevcut mu?	SOC, tehditlerin erken tespiti ve hızlı müdahale ile güvenlik risklerini azaltır; SOC olmadan, saldırılar geç fark edilip daha büyük zararlara yol açabilir. SOC'nin etkinliği, düzenli olarak gerçekleştirilen Red Teaming ve sızma testleriyle değerlendirilmelidir.
	8.4 Sızma Testleri (Penetrasyon Testleri)	Sızma testleri, bir kuruluşun bilgi sistemlerindeki güvenlik açıklarını tespit etmek amacıyla, yetkilendirilmiş uzmanlar tarafından gerçekleştirilen kontrollü saldırı simülasyonlarıdır. Bu testler, sistemlerin mevcut güvenlik durumunu değerlendirerek, potansiyel zafiyetleri belirlemeyi hedefler.	Şirketimizin bilgi sistemleri düzenli olarak sızma testlerine tabi tutuluyor mu?	Sızma testleri, sistemlerdeki güvenlik açıklarını proaktif olarak belirleyip gidermeye yardımcı olur. Bu testlerin ihmal edilmesi, saldırganların bu zafiyetlerden yararlanmasına ve potansiyel veri ihlallerine yol açabilir. Sızma testlerinin ardından, daha kapsamlı güvenlik değerlendirmeleri için Red Teaming faaliyetleri gerçekleştirilmelidir.
	8.5 Red Teaming	Red Teaming, organizasyonun güvenlik savunmalarını, gerçek dünya saldırı senaryolarını simüle ederek kapsamlı bir şekilde test eden bir yaklaşımdır. Bu yöntem, sadece teknik sistemleri değil, aynı zamanda insan faktörünü ve süreçleri de değerlendirerek, savunma mekanizmalarının bütüncül bir analizini sağlar.	Organizasyonumuz, güvenlik savunmalarını değerlendirmek için düzenli olarak Red Teaming egzersizleri yapıyor mu?"	Red Teaming, saldırganların kullanabileceği taktik, teknik ve prosedürleri (TTP) kullanarak, organizasyonun savunma mekanizmalarını gerçekçi bir şekilde test eder. Bu sayede, güvenlik açıkları ve zayıf noktalar proaktif olarak belirlenir ve giderilir. Red Teaming'in ihmal edilmesi, organizasyonun güvenlik duruşunun eksik değerlendirilmesine ve potansiyel tehditlere karşı savunmasız kalmasına neden olabilir. Red Teaming faaliyetleri sonrasında tespit edilen güvenlik olaylarının detaylı analizi ve delillendirilmesi için Dijital Adli Bilişim ve Soruşturma süreçleri devreye alınmalıdır.
	8.6 Dijital Adli Bilişim ve Soruşturma	Dijital adli bilişim, siber olayların izlerini sürmek, delil toplamak ve analiz etmek için kullanılan yöntemler bütünüdür.	Şirketimizde siber olayların adli analizi ve soruşturması için gerekli yetkinlik ve araçlar mevcut mu?	Dijital adli bilişim, olayların kökenini anlamak ve gelecekte benzer saldırıları önlemek için kritiktir; bu süreçlerin eksikliği, saldırıların tekrarlanmasına ve yasal sorunlara yol açabilir.

9.0 Endüstriyel ve IoT Güvenliği

	9.0 Endüstriyel ve IoT Güvenliği	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	9.1 Endüstriyel Kontrol Sistemi (ICS) Güvenliği	Endüstriyel Kontrol Sistemleri (ICS), endüstriyel süreçlerin yönetimi ve otomasyonu için kullanılan cihazlar, sistemler ve ağların bütünüdür.	ICS altyapımızın güvenliği düzenli olarak değerlendiriliyor ve güncelleniyor mu?	ICS güvenliği, enerji santralleri ve üretim tesisleri gibi kritik altyapıların korunması için hayati öneme sahiptir; bu sistemlerin güvenliğinin ihmal edilmesi, üretim kazalarına ve büyük ölçekli kesintilere yol açabilir. ICS güvenliğinin sağlanması, OT güvenliği ile doğrudan ilişkilidir ve entegre bir yaklaşım gerektirir.
	9.2 OT Güvenliği	Operasyonel Teknoloji (OT) güvenliği, endüstriyel operasyonları yöneten donanım ve yazılım sistemlerinin korunmasına odaklanır.	OT sistemlerimizin güvenlik açıkları düzenli olarak tespit edilip gideriliyor mu?	OT güvenliği, üretim süreçlerinin kesintisiz ve güvenli bir şekilde devam etmesini sağlar; ihmal edilmesi durumunda, siber saldırılar üretim hatlarında durmalara ve ciddi ekonomik kayıplara neden olabilir. OT güvenliğinin güçlendirilmesi, akıllı şebeke sistemlerinin korunması için de temel bir adımdır.
	9.3 Akıllı Şebeke Güvenliği	Akıllı şebeke güvenliği, enerji dağıtım ağlarının dijital bileşenlerinin ve iletişim altyapısının korunmasına yönelik uygulamaları içerir.	Akıllı şebeke altyapımızın siber tehditlere karşı dayanıklılığı nasıl sağlanıyor?	Akıllı şebekelerin güvenliği, enerji arzının sürekliliği ve güvenilirliği için kritik öneme sahiptir; güvenlik açıkları, geniş çaplı elektrik kesintilerine ve ekonomik zararlara yol açabilir. Bu güvenlik önlemleri, IoT cihazlarının entegrasyonuyla daha da karmaşık hale gelen tehditleri yönetmek için gereklidir.
	9.4 IoT Güvenliği ve Tehdit Algılama	IoT güvenliği, internete bağlı cihazların ve ağların korunmasına yönelik stratejileri ve tehdit algılama mekanizmalarını kapsar. Kontrol Sorusu:	IoT cihazlarımızın güvenliği ve olası tehditlerin tespiti için hangi önlemleri alıyoruz?	IoT cihazları, zayıf şifreler veya güncellenmemiş yazılımlar nedeniyle siber saldırılara karşı savunmasız olabilir; bu da veri ihlallerine ve hizmet kesintilerine yol açabilir. Etkili bir IoT güvenlik stratejisi, tüm endüstriyel ve operasyonel sistemlerin bütünsel güvenliği için temel teşkil eder.

10.0 Bulut Güvenliği

	10.0 Bulut Güvenliği	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	10.1 Web Uygulama Güvenlik Duvarı (WAF)	Web Uygulama Güvenlik Duvarı (WAF), web uygulamalarını SQL enjeksiyonu, XSS ve diğer saldırılara karşı koruyan bir güvenlik önlemidir.	Web uygulamalarımızın önünde etkin bir WAF çözümü bulunuyor mu?	WAF, web uygulamalarını hedef alan saldırıları engelleyerek veri ihlallerini ve hizmet kesintilerini önler; bu tür saldırılar, müşteri güvenini sarsabilir ve yasal sorunlara yol açabilir. WAF kullanımı, API güvenliği ile entegre edilerek daha kapsamlı bir koruma sağlar.
	10.2 API Güvenliği	API güvenliği, uygulamalar arasındaki veri alışverişini sağlayan arayüzlerin yetkisiz erişim ve saldırılara karşı korunmasını içerir.	Tüm API'lerimiz kimlik doğrulama ve yetkilendirme mekanizmalarıyla korunuyor mu?	API'ler, hassas verilere erişim noktalarıdır ve güvenlik açıkları, veri sızıntılarına ve sistem bütünlüğünün bozulmasına neden olabilir; bu da şirketin itibarını ve müşteri güvenini zedeler. API güvenliği, uygulama güvenlik testleri ile desteklenerek daha sağlam bir yapı oluşturulabilir.
	10.3 Uygulama Güvenlik Testleri	Uygulama güvenlik testleri, yazılımların güvenlik açıklarını belirlemek ve gidermek amacıyla yapılan değerlendirmelerdir.	Uygulamalarımız düzenli olarak güvenlik testlerinden geçiriliyor mu?	Güvenlik testleri, potansiyel zafiyetleri proaktif olarak tespit ederek saldırı riskini azaltır; ihmal edilmesi, saldırganların bu açıkları istismar etmesine yol açabilir. Bu testler, kod inceleme ve statik analiz süreçleriyle tamamlanmalıdır.
	10.4 Kod İnceleme & Statik Analiz	Kod inceleme ve statik analiz, yazılım kodunun manuel veya otomatik araçlarla incelenerek güvenlik açıklarının tespit edilmesi sürecidir.	Kodlarımız düzenli olarak güvenlik açısından inceleniyor ve analiz ediliyor mu?	Bu süreçler, yazılım geliştirme aşamasında güvenlik açıklarını erkenden belirleyerek maliyetli düzeltmelerin ve olası güvenlik ihlallerinin önüne geçer; aksi takdirde, üretim ortamında ciddi güvenlik sorunları ortaya çıkabilir. Güvenli kodlama uygulamalarının benimsenmesi, bu analizlerin etkinliğini artırır.
	10.5 Güvenli Kodlama Uygulamaları	Güvenli kodlama uygulamaları, yazılım geliştiricilerin güvenlik açıklarını önlemek için takip ettiği en iyi uygulamalar ve standartlardır.	Geliştiricilerimiz güvenli kodlama standartlarına uygun şekilde çalışıyor mu?	Güvenli kodlama, yazılımın dayanıklılığını artırır ve saldırı yüzeyini azaltır; ihmal edilmesi, yazılımın savunmasız hale gelmesine ve saldırılara açık olmasına neden olabilir. Bu uygulamalar, güvenli yazılım geliştirme yaşam döngüsünün temelini oluşturur.
	10.6 Güvenli Yazılım Geliştirme	Güvenli yazılım geliştirme, yazılımın tasarımından dağıtımına kadar tüm aşamalarda güvenlik önlemlerinin entegre edilmesini içerir.	Yazılım geliştirme süreçlerimizde güvenlik, baştan sona entegre edilmiş mi?	Bu yaklaşım, güvenlik açıklarını erken aşamada tespit ederek düzeltme maliyetlerini düşürür ve yazılımın güvenilirliğini artırır; aksi halde, sonradan tespit edilen güvenlik açıkları daha büyük riskler ve maliyetler doğurabilir. DevSecOps metodolojisi, bu süreci daha da etkin hale getirir.
	10.7 DevSecOps	DevSecOps, yazılım geliştirme ve operasyon süreçlerine güvenliği entegre ederek, güvenlik açıklarını erken aşamada tespit etmeyi amaçlayan bir metodolojidir.	Yazılım geliştirme ve operasyon süreçlerimizde güvenlik, başlangıçtan itibaren entegre edildi mi?	DevSecOps, güvenlik açıklarını erken tespit ederek yazılım geliştirme süreçlerini hızlandırır ve daha güvenli ürünler ortaya çıkarır; aksi takdirde, güvenlik zafiyetleri geç fark edilerek maliyetli ve zaman alıcı düzeltmelere yol açabilir.
	10.8 Konteyner Güvenliği	Konteyner güvenliği, konteyner tabanlı uygulamaların ve altyapının güvenliğini sağlamak için alınan önlemleri kapsar.	Konteyner tabanlı uygulamalarımızın güvenliği için gerekli önlemleri aldık mı?	Konteynerlerin güvenliği sağlanmadığında, saldırganlar sistemlere sızabilir ve hassas verilere erişebilir; bu da veri ihlallerine ve hizmet kesintilerine yol açabilir.
	10.9 Mobil Güvenlik	Mobil güvenlik, mobil cihazlar ve uygulamaların yetkisiz erişim, veri sızıntısı ve kötü amaçlı yazılımlara karşı korunmasını içerir.	Mobil uygulamalarımızın güvenliği düzenli olarak test ediliyor ve güncelleniyor mu?	Mobil cihazlar ve uygulamalar, siber saldırganlar için cazip hedeflerdir; güvenlik önlemleri alınmadığında, veri sızıntıları ve yetkisiz erişimler yaşanabilir, bu da müşteri güvenini ve şirket itibarını zedeler.

11.0 İleri Düzey Bulut Güvenliği

	11.0 İleri Düzey Bulut Güvenliği	Nedir?	Kontrol Sorusu	Riskler Nedir ve Neden Kullanılmalı?
	11.1 Bulut Güvenlik Duruşu Yönetimi (CSPM)	CSPM, bulut ortamlarındaki güvenlik yapılandırmalarını sürekli izleyerek yanlış yapılandırmaları ve uyumsuzlukları tespit eden bir süreçtir.	Bulut altyapımızın güvenlik yapılandırmaları düzenli olarak denetleniyor ve uyumluluk sağlanıyor mu?	Yanlış yapılandırılmış bulut kaynakları, veri ihlallerine ve uyumluluk sorunlarına yol açabilir; CSPM, bu riskleri azaltarak güvenlik duruşunu güçlendirir.
	11.2 Bulut Kimlik ve Erişim Yönetimi (Cloud IAM)	Cloud IAM, bulut ortamlarında kullanıcıların ve hizmetlerin kimliklerini yöneterek, doğru kaynaklara uygun erişim seviyelerini sağlar.	Bulut kaynaklarımıza erişim yetkileri, kullanıcı rollerine göre doğru şekilde tanımlandı ve düzenli olarak gözden geçiriliyor mu?	Yanlış yapılandırılmış erişim kontrolleri, yetkisiz erişimlere ve veri sızıntılarına neden olabilir; Cloud IAM, güvenli ve kontrollü erişim sağlayarak bu riskleri minimize eder.
	11.3 Bulut İş Yükü Koruma (CWP)	CWP, bulut tabanlı iş yüklerini tehditlere karşı koruyan ve güvenlik politikalarını uygulayan bir çözümdür.	Bulut iş yüklerimiz, kötü amaçlı aktiviteler ve güvenlik açıklarına karşı etkin bir şekilde izleniyor ve korunuyor mu?	Bulut ortamlarında çalışan iş yükleri, çeşitli tehditlere maruz kalabilir; CWP, bu iş yüklerini koruyarak veri bütünlüğünü ve hizmet sürekliliğini sağlar.
	11.4 Cloud Native Güvenliği	Cloud Native güvenliği, bulut tabanlı uygulamaların tüm yaşam döngüsü boyunca güvenliğini sağlamayı hedefleyen bir yaklaşımdır.	Bulut tabanlı uygulamalarımızın geliştirme, dağıtım ve işletim süreçlerinde güvenlik önlemleri entegre edildi mi?	Bulutun dinamik yapısı, geleneksel güvenlik yöntemlerinin yetersiz kalmasına neden olabilir; Cloud Native güvenliği, bu ortamların özelliklerine uyum sağlayarak güvenlik standartlarını korur.
	11.5 Kubernetes Güvenliği	Kubernetes güvenliği, Kubernetes ortamlarında çalışan konteynerlerin ve altyapının korunmasına yönelik uygulamaları içerir.	Kubernetes kümelerimizde erişim kontrolleri, ağ politikaları ve güvenlik yamaları düzenli olarak uygulanıyor mu?	Kubernetes'in karmaşık yapısı, güvenlik açıklarına yol açabilir; uygun güvenlik önlemleri alınmadığında, saldırganlar sistemlere sızabilir ve hizmetleri aksatabilir.
	11.6 Sunucusuz Güvenlik (Serverless Security)	Sunucusuz güvenlik, sunucusuz mimarilerde çalışan uygulamaların ve işlevlerin güvenliğini sağlamaya yönelik önlemleri kapsar.	Sunucusuz uygulamalarımızın güvenlik açıkları düzenli olarak değerlendiriliyor ve gerekli önlemler alınıyor mu?"	Sunucusuz mimariler, altyapı yönetimini basitleştirirken yeni güvenlik riskleri de getirir; bu risklerin yönetilmemesi, veri ihlallerine ve hizmet kesintilerine yol açabilir.

0’dan 82’ye Siber Güvenlik

Aşağıdaki listelenen verilerle birlikte **0’dan 82’e Siber Güvenlik** raporunun premium versiyonu için bize ulaşın - team@pitgrowth.com

- Çözümleri Hangi Tür İşletmeler Kullanmalı?*
- Çözümleri Hangi Endüstriler Kullanmalı?*
- Çözümler Kaç Çalışanlı Şirketler İçin Uygun?*
- Çözümler Şirketler İçin Temel Gereklilik mi?*
- Türkiye’de Hangi Şirketlerin Ürünleri Var?*

Not: İşaretli * detaylar için kurumsal üyelik gereklidir.