



Privia
SECURITY



Altyapı ve Mimari Gözden Geçirme Hizmeti

Profesyonel Defensive Security Hizmetleri

“İyi Bir Savunma İyi Bir Mimari ile Başlar!”

Bu dokümanda yer alan bilgiler Privia Security Bilişim ve Danışmanlık Hizmetleri A.Ş. tarafından gerçekleştirilen Defensive Hizmetlere ait bilgiler olup **Genel** mahiyetindedir. Bu dokümanda yer alan tüm bilgiler, kamuya açıktır.

Küçükbakkalköy Mah. Kocasinan Cad.
Privia Plaza No:42 Ataşehir, İstanbul

+90 (216) 514 72 14

www.priviasecurity.com

Dok. Kodu	DefSec-00222/TR
Tarih	06.01.2025
Revizyon Tar.	-
Versiyon	1.0.0
Gizlilik	Genel

“Güçlü bir altyapı mimarisi, organizasyonun dijital/endüstriyel varlıklarını koruma altına alarak kesintisiz iş sürekliliği sağlar. Gözden geçirme süreci, tüm bileşenlerin güvenlik standartlarına uyumunu denetler ve güvenlik politikalarının etkinliğini artırır.”

Altyapı ve Mimari Gözden Geçirme Hizmeti, organizasyonların dijital altyapılarını ve güvenlik mimarilerini analiz ederek güvenlik standartlarına (secure-by-design) uygun hale getirmeyi hedefler. Hizmet altyapı zafiyetleri, konfigürasyon hataları, mimari analiz, teknoloji ve politika incelemesi gibi analiz süreçlerini kapsar. Problemlerin tespiti, mimari yapıların optimizasyonu ve güvenlik stratejilerinin geliştirilmesi hizmetin en önemli bileşenlerindedir.

Altyapı güvenliği ve mimari gözden geçirme sürecinde, organizasyonların operasyonel hedeflerine uygun çözümler sunulmaktadır. Siber tehditlerin gelişen yapısı, altyapı güvenliğinin güncellenmesini ve uyumlu hale getirilmesini zorunlu kılar. Güvenlik mimarisi ile altyapının kapsamlı bir şekilde değerlendirilmesi, organizasyonların dijital güvenliğini sürdürülebilir kılmak adına önemlidir. Hizmet kapsamı detaylandırılarak her organizasyona özel stratejiler geliştirilmektedir. Gözden geçirme süreci, altyapı zafiyetlerinin analiz edilmesi ve riskli noktaların belirlenmesi ile başlar. Tespit edilen problemler, detaylı raporlarla ilgili ekiplere sunularak çözüm önerileriyle birlikte paylaşılır. Altyapıdaki her bileşen için güvenlik standartlarına uygun optimizasyon çalışmaları yapılır. Altyapının güvenliği, düzenli analizler ve güncellemeler ile sürekli olarak desteklenir.

Altyapı ve Mimari Gözden Geçirme Hizmeti, organizasyonların güvenlik standartlarına uygun altyapı kurmasına olanak tanır. Güvenli ve dayanıklı bir altyapı, operasyonel verimliliği artırırken siber tehditlere karşı güçlü bir savunma oluşturur.

Dok. Kodu	DefSec-00222/TR
Tarih	06.01.2025
Revizyon Tar.	-
Versiyon	1.0.0
Gizlilik	Genel

Hizmete Ait Bileşenler

Acil Eylem Planının Çıkartılması

Acil eylem planı, organizasyonun güvenlik altyapısını güçlendirmek ve hızlı müdahale kabiliyetini artırmak için gereken adımları içerir. Organizasyonun en yüksek risk taşıyan varlıklarını ve altyapı bileşenlerini analiz ederek acil müdahale gerektiren alanları saptar. Acil Eylem Planı kapsamında, tehditlerin minimize edilmesi için hızlıca uygulanabilecek güvenlik stratejileri oluşturulur. Organizasyonun ihtiyaçlarına göre özelleştirilen plan, tehditlerin yayılmasını engelleyecek teknolojik yatırımları ve iyileştirmeleri içerir. Eylem planı, güvenlik zafiyetlerine karşı çözümler sunar ve altyapı güvenliğini güçlendirir. Planın uygulanması, güvenlik ekiplerinin tehditlere hızlı yanıt vermesini kolaylaştırır.

Mevcut Kontrollerin Değerlendirilmesi

Mevcut kontrollerin değerlendirilmesi, organizasyonun mevcut güvenlik önlemlerinin etkinliğini analiz etmek için gerçekleştirilir. Mevcut altyapıdaki güvenlik çözümlerini detaylı bir şekilde gözden geçirilir ve iyileştirme gerektiren alanlar belirlenir. Gerçekleştirilen değerlendirme, organizasyonun dijital varlıklarının korunması için gerekli önlemleri tanımlar. Mevcut güvenlik çözümlerinin etkinliği, yeni tehditlere karşı güncel olup olmadığıyla birlikte analiz edilir. Teknik kontrol değerlendirmeleri, güvenlik altyapısının zayıf noktalarını ve güvenlik zafiyetlerini belirlemeye odaklanır. Eksik veya yetersiz kontroller tespit edilerek gerekli güncellemelerin yapılması sağlanır.

Orta Vadeli Teknoloji Planlanması

Orta vadeli güvenlik projeleri, organizasyonun altyapı güvenliğini daha ileriye taşıyacak stratejik adımları kapsar. Projeler organizasyonun dijital güvenliğini sürdürülebilir kılabilecek güvenlik çözümlerini ve teknolojik altyapıları içerir. Güvenlik ekipleri, ihtiyaç analizine dayalı olarak güvenlik projelerini belirler ve önceliklendirir. Organizasyonun sektörel gereksinimlerine ve tehdit ortamına uygun çözüm ve teknolojiler projelendirilir. Orta vadeli projeler, güvenlik altyapısının gelişen tehditlere karşı güncel ve güçlü kalmasını sağlar.

İzleme Altyapısının Geliştirilmesi

İzleme ve alarm altyapısı, organizasyonun güvenlik olaylarını anlık olarak takip edip tehditleri erkenden tespit etmesini sağlar. Güvenlik ekipleri, altyapıdaki şüpheli aktiviteleri izleyerek güvenlik olaylarına anında müdahale eder. Alarm sistemleri, tehditlerin erkenden tespit edilmesi için optimize edilir ve altyapının her alanını kapsayacak şekilde yapılandırılır. Güvenlik zafiyetlerinin minimize edilmesi için alarm altyapısı sürekli güncellenir ve test edilir. İzleme çözümleri, organizasyonun güvenlik durumunu gerçek zamanlı kontrol altında tutarak riskleri azaltır. Güçlü bir izleme ve alarm altyapısı, güvenlik açıklarının oluşmasını önlemeye katkı sunar.

Dok. Kodu	DefSec-00222/TR
Tarih	06.01.2025
Revizyon Tar.	-
Versiyon	1.0.0
Gizlilik	Genel

Kapsamlı Envanter Çalışması

Dijital varlık yönetimi, organizasyonun altyapısındaki tüm dijital kaynakları güvenli bir şekilde kontrol altında tutmayı amaçlar. Kapsamlı envanter çalışması, mevcut altyapı bileşenlerinin detaylı bir listesinin çıkarılmasını içerir. Güvenlik ekipleri, organizasyonun dijital varlıklarının mevcut güvenlik durumunu ve eksiklerini analiz eder. Envanter çalışması, güvenlik stratejilerinin daha etkili uygulanmasına katkı sunar. Dijital varlık yönetimi, varlıkların korunması için düzenli olarak güncellenir ve izlenir. Güvenlik açıklarının oluşmaması için varlıklar sürekli olarak kontrol altında tutulur. Organizasyon, hangi varlıkların güvenlik önlemlerine ihtiyaç duyduğunu net bir şekilde görür.

Zafiyet Yönetimi

Sürekli güvenlik testleri, altyapıda meydana gelebilecek yeni güvenlik açıklarının tespit edilmesi için düzenli olarak gerçekleştirilir. Güvenlik ekiplerimiz sistemlerdeki güvenlik zafiyetlerini belirlemek için kapsamlı test süreçleri uygular. Zafiyet yönetimi, tespit edilen güvenlik açıklarının kapatılması ve altyapının güvenlik seviyesinin iyileştirilmesini sağlar. Hizmet, organizasyonun güvenlik açıklarına karşı sürekli koruma altında kalmasını sağlar. Güvenlik testleri, organizasyonun güvenlik politikaları ve standartlarına uyumlu bir şekilde yürütülür. Zafiyet yönetimi, güvenlik açıklarının kök nedenini analiz ederek gelecekteki tehditlerin önlenmesini amaçlar.

Dok. Kodu	DefSec-00222/TR
Tarih	06.01.2025
Revizyon Tar.	-
Versiyon	1.0.0
Gizlilik	Genel

Sık Sorulan Sorular

Altyapı ve Mimari Gözden Geçirme Hizmeti nedir ve organizasyonlara nasıl fayda sağlar?

Altyapı ve Mimari Gözden Geçirme Hizmeti, organizasyonların dijital mimarisini güvenlik standartlarına uygun hale getirmeyi amaçlayan kapsamlı bir analiz sürecidir. Altyapı zafiyetlerinin, konfigürasyon hatalarının ve güvenlik politikalarının detaylı bir şekilde değerlendirilmesini içerir. Organizasyonların mevcut güvenlik durumu incelenerek iyileştirme alanları belirlenir ve uygun stratejiler oluşturulur. Altyapıdaki riskli noktalar belirlenip çözüm önerileri sunulur ve altyapı iyileştirilir. Hizmet, organizasyonun operasyonel verimliliğini destekler ve siber tehditlere karşı daha güçlü bir altyapı sağlar.

Altyapı gözden geçirme süreci nasıl işler?

Gözden geçirme süreci, organizasyonun mevcut altyapısının detaylı bir analizini yapmakla başlar. İlk aşamada altyapı bileşenleri ve ağ yapılandırmaları gibi teknik unsurlar gözden geçirilerek güvenlik zafiyetleri tespit edilir. Mevcut güvenlik kontrollerinin etkinliği değerlendirilip iyileştirme gerektiren alanlar belirlenir. İkinci aşamada, tespit edilen zafiyetler detaylı raporlarla sunulur ve çözüm önerileri güvenlik ekiplerine iletilir. Ayrıca acil eylem planı oluşturularak güvenlik önlemlerinin hızlıca hayata geçirilmesi sağlanır.

Bu hizmeti kimler almalıdır ve hangi sektörler için uygundur?

Altyapı ve Mimari Gözden Geçirme Hizmeti, dijital/endüstriyel varlıklarını ve altyapı güvenliğini koruma ihtiyacı hisseden tüm organizasyonlar için uygundur. Özellikle finans, sağlık, enerji, üretim, kamu ve telekomünikasyon gibi hassas verilerin işlendiği sektörlerde bu hizmet kritik öneme sahiptir. Aynı zamanda hızlı bir şekilde güvenlik önlemlerini artırmak ve altyapıyı sürdürülebilir hale getirmek isteyen firmalar için de idealdir. Hizmet, tüm sektörler için esnek ve uyarlanabilir çözümler sunar.

Altyapı güvenliğinin sağlanması neden önemlidir?

Altyapı güvenliği, organizasyonun dijital/endüstriyel varlıklarının siber saldırılara karşı korunması için kritik bir öneme sahiptir. Güvenli bir altyapı, organizasyonun verilerini ve operasyonel süreçlerini iç/dış tehditlerden korur. Güçlü bir altyapı güvenliği, organizasyonun operasyonel sürekliliğini destekler ve kesintisiz bir çalışma ortamı sağlar. Altyapıda bulunan güvenlik zafiyetlerinin giderilmesi, siber saldırı riskini minimize eder ve veri ihlallerinin önlenmesini sağlar.

Altyapı ve Mimari Gözden Geçirme Hizmeti ile hangi güvenlik açıkları tespit edilir?

Hizmet, organizasyonun dijital altyapısındaki çeşitli güvenlik zafiyetlerini tespit ederek çözüm önerileri sunar. Zayıf parola politikaları, eksik güncellemeler, yetersiz erişim kontrolleri ve yanlış yapılandırmalar gibi zafiyetler analiz edilir. Ayrıca güvenlik

Dok. Kodu	DefSec-00222/TR
Tarih	06.01.2025
Revizyon Tar.	-
Versiyon	1.0.0
Gizlilik	Genel

protokollerine uyum eksiklikleri ve tehditlerin izlenmesi gibi riskler de değerlendirilir. Altyapıda yer alan cihazlar, ağ yapılandırmaları ve güvenlik politikaları detaylı bir şekilde incelenir. Hizmet, altyapıdaki her bir bileşenin güvenlik standartlarına uygunluğunu denetleyerek eksiklerin giderilmesini sağlar.

Bu hizmetin sunduğu acil eylem planı nedir ve nasıl uygulanır?

Acil eylem planı, organizasyonun güvenlik altyapısını hızlıca güçlendirmek için gerekli adımları belirleyen bir strateji planıdır. Plan kapsamında, organizasyonun en yüksek risk taşıyan varlıkları analiz edilip acil müdahale gerektiren alanlar tespit edilir. Güvenlik ekipleri, tespit edilen zafiyetlere karşı etkili güvenlik stratejileri geliştirir ve uygulamaya alır. Acil eylem planı, güvenlik olaylarına hızlı müdahale edilmesini sağlar. Güvenlik önlemlerinin etkili bir şekilde hayata geçirilmesi için yapılması gereken yatırımları ve teknik çözümleri içerir. Güvenlik ekipleri, acil durumlarda plan doğrultusunda hareket ederek tehditleri minimize eder.

Altyapı ve Mimari Gözden Geçirme Hizmeti'nin yasal uyumluluğa katkısı nedir?

Altyapı ve Mimari Gözden Geçirme Hizmeti, organizasyonların yasal gereksinimlere ve güvenlik standartlarına uygun bir altyapı kurmalarını sağlar. Hizmet kapsamında uygulanan güvenlik çözümleri, veri güvenliği yasalarına ve sektörel düzenlemelere uyum sağlamayı kolaylaştırır. Güvenlik politikaları, yasal gereklilikler doğrultusunda güncellenir ve denetimlerde istenen güvenlik standartlarına uygun hale getirilir. Altyapı güvenliği ile ilgili eksikliklerin giderilmesi, organizasyonun yasal sorumluluklarını yerine getirmesine katkıda bulunur.

Siber Güvenlikte Doğru Çözüm Ortağınız

2018 yılında siber güvenliğin geleceği için yola çıkan Privia Security, kuruluşundan bu yana, müşterilerine yüksek kaliteli hizmet sunmayı amaçlamaktadır. Güçlü ve yetenekli ekibimiz, siber güvenliğin her alanında hizmet verdiğimiz organizasyonlara en güvenilir ve kapsamlı çözümleri sunarak, organizasyonların dijital dünyadaki güvenlik ihtiyaçlarını karşılamaktadır.

Günümüzde hızla gelişen ve karmaşık hale gelen siber tehditlerle mücadele etmek giderek zorlaşıyor. Bu noktada Privia Security olarak, müşterilerimize ihtiyaç duydukları hem defansif hem de ofansif siber güvenlik stratejilerini en ileri teknolojiyle sunuyoruz. İnovatif AR-GE ürünlerimiz ve stratejik danışmanlığımız sayesinde organizasyonların siber güvenlik olgunluğunu artırmayı ve onlara proaktif çözümler sunmayı hedefliyoruz. Şu anda 300'den fazla büyük kuruluşun güvenliğini sağlamaktan gurur duyuyoruz.

Uluslararası ve Yerel Siber Güvenlik Çözümleri

Privia Security olarak, Avrupa, Asya, Ortadoğu ve Amerika dahil olmak üzere geniş bir coğrafyaya siber güvenlik hizmetleri sunmaktayız. Offensive, Defensive ve Forensic alanlarında uzmanlaşmış ekiplerimiz, kritik altyapılar, aviyonik sistemler, kurumsal ağlar ve askeri alanlar gibi farklı sektörlerde faaliyet gösteren organizasyonlara özel çözümler geliştirmektedir.

Ayrıca savunma kapasitelerini güçlendirmek isteyen ülkelere yönelik geliştirdiğimiz PriviaHub siber savaş simülasyonu ile siber savaş stratejilerinin test edilmesi, tatbikatların yürütülmesi ve uzmanların niteliklerinin ölçülmesi için kapsamlı çözümler sunuyoruz. Bu inovatif platform özel sektör, akademi ve askeri alanlarda tatbikat ihtiyaçlarını karşılamak üzere tasarlanmıştır.

İleri Teknoloji ile Güvenli Gelecek

İstanbul, Ankara, Londra ve Cumhuriyet Teknopark'taki Ar-Ge merkezimizde, müşterilerimize değer katan projeler geliştiriyoruz. Penetrasyon testleri, Red Team operasyonları, siber güvenlik eğitimleri ve kurumlara özel siber güvenlik çözümlerimizle sektörde fark yaratmaya devam ediyoruz. "Privacy For You" sloganımızla, güvenlik ve gizliliğe yenilikçi bir bakış açısı getiriyor ve müşterilerimizin dijital geleceğini güvence altına alıyoruz.

