EMA SECURITY

Siber Olgunluk Hizmeti

AI-Powered Defense Service

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Hizmet Tanımı

Siber Olgunluk ve Risk Değerlendirme Hizmeti, kuruluşların mevcut siber güvenlik durumunu kapsamlı bir şekilde analiz ederek riskleri belirlemeye ve olgunluk seviyesini artırmaya yönelik stratejik bir güvenlik çözümüdür. Günümüzde gelişen tehdit ortamı ve sıkılaşan regülasyonlar, organizasyonların siber güvenlik seviyelerini sürekli olarak değerlendirmelerini ve iyileştirmelerini zorunlu hale getirmektedir. Bu hizmet, kuruluşların güvenlik açıklarını tespit etmelerine, kritik varlıklarını korumalarına ve risk yönetimi süreçlerini güçlendirmelerine yardımcı olur.

Hizmet kapsamında, organizasyonun mevcut güvenlik politikaları, süreçleri, teknolojik altyapısı ve çalışan farkındalığı detaylı bir şekilde incelenir. NIST Cybersecurity Framework (CSF), ISO 27001, CIS Controls ve diğer uluslararası güvenlik standartlarına uygun bir değerlendirme yapılır. Siber olgunluk seviyesi, belirlenen güvenlik çerçeveleri ile karşılaştırılarak organizasyonun güçlü ve zayıf yönleri belirlenir. Kritik güvenlik kontrolleri, tehdit yüzeyi analizi, saldırı vektörleri ve potansiyel risk senaryoları değerlendirilerek kapsamlı bir risk analizi gerçekleştirilir.

Bu süreçte, varlık envanteri oluşturularak korunması gereken sistemler belirlenir, tehdit modelleme çalışmaları yapılarak organizasyona özgü risk faktörleri analiz edilir ve güvenlik açıkları önceliklendirilir. Siber güvenlik risk yönetimi kapsamında, tehditlerin potansiyel etkileri değerlendirilerek risk azaltma stratejileri belirlenir. Güvenlik açıklarının giderilmesi, uygun güvenlik önlemlerinin uygulanması ve riskin kabul edilebilir seviyeye düşürülmesi için bir yol haritası oluşturulur.

Ayrıca, organizasyon çalışanlarının siber güvenlik farkındalık seviyeleri değerlendirilir ve bilinçlendirme çalışmaları planlanır. Güvenlik süreçleri, olay müdahale yetkinlikleri, veri koruma politikaları ve erişim yönetimi mekanizmaları gözden geçirilerek olgunluk seviyesi artırılacak alanlar belirlenir. Kuruluşun güvenlik duruşunun sürekli iyileştirilmesi için düzenli değerlendirmeler yapılır ve güvenlik stratejileri dinamik tehdit ortamına uygun şekilde güncellenir.

Siber Olgunluk ve Risk Değerlendirme Hizmeti, kuruluşların siber güvenlik risklerini yönetmelerine, yasal ve sektörel uyumluluk gereksinimlerini karşılamalarına ve güvenlik süreçlerini sürekli geliştirmelerine yardımcı olur. Bu sayede organizasyonlar, siber saldırılara karşı daha dirençli hale gelirken, operasyonel sürekliliklerini ve güvenilirliklerini koruma konusunda önemli bir avantaj elde ederler.

Hizmete Ait Bileşenler

Mevcut Güvenlik Duruşu Analizi

Kuruluşun mevcut güvenlik politikaları, süreçleri, teknolojik altyapısı ve siber güvenlik yetkinlikleri değerlendirilir. Güvenlik açıkları, tehdit yüzeyi ve saldırı vektörleri analiz edilerek mevcut risk profili çıkarılır.

Varlık Envanteri ve Değerleme

Tüm bilgi varlıkları belirlenerek sistemler, uygulamalar, veri tabanları ve ağ bileşenleri envanterlenir. Kritik varlıkların korunması için önceliklendirme yapılır ve risk seviyeleri belirlenir.

Tehdit Modelleme ve Risk Analizi

Olası tehdit aktörleri, saldırı senaryoları ve organizasyona özgü risk faktörleri analiz edilir. Risk analizi kapsamında saldırı olasılığı ve potansiyel etkileri değerlendirilerek tehditlerin önceliklendirilmesi sağlanır.

Uyumluluk ve Regülasyon Değerlendirmesi

ISO 27001, NIST CSF, CIS Controls, GDPR, KVKK ve sektörel regülasyonlar gibi uluslararası ve yerel uyumluluk çerçevelerine göre kuruluşun güvenlik durumu değerlendirilir. Eksiklikler tespit edilerek yasal uyumluluk planları oluşturulur.

Güvenlik Açıkları ve Kontrollerin Değerlendirilmesi

Mevcut güvenlik kontrolleri incelenerek güvenlik açıkları tespit edilir. Güçlü kimlik doğrulama, erişim yönetimi, ağ güvenliği, veri şifreleme, olay yönetimi gibi kritik güvenlik mekanizmalarının yeterliliği değerlendirilir.

Olay Müdahale ve Kriz Yönetimi Yetkinlikleri

Olay müdahale süreçleri, güvenlik operasyon merkezi (SOC) yetkinlikleri ve kriz yönetim prosedürleri analiz edilir. Olası bir siber saldırıya karşı organizasyonun ne kadar hızlı ve etkin yanıt verebileceği değerlendirilir.

Güvenlik Farkındalık ve Eğitim Değerlendirmesi

Çalışanların siber güvenlik farkındalık düzeyi ölçülerek bilinçlendirme programları belirlenir. Sosyal mühendislik saldırılarına karşı organizasyonun ne kadar dirençli olduğu test edilerek eğitim stratejileri oluşturulur.

Risk Azaltma ve Güvenlik Stratejileri Belirleme

Tespit edilen güvenlik açıklarına yönelik risk azaltma planları oluşturulur. Önerilen güvenlik iyileştirmeleri ile organizasyonun siber olgunluk seviyesinin artırılması hedeflenir.

Sürekli İzleme ve Geliştirme

Siber tehdit ortamı dinamik olduğu için düzenli güvenlik değerlendirmeleri ve olgunluk analizleri yapılır. Risk yönetim süreçleri sürekli iyileştirilerek güvenlik stratejileri güncellenir.

Siber Olgunluk ve Risk Değerlendirme Metodolojisi

Siber Olgunluk ve Risk Değerlendirme Hizmeti, kuruluşların mevcut siber güvenlik seviyesini analiz ederek, riskleri minimize edecek stratejik önlemler geliştirmeyi amaçlayan kapsamlı bir süreçtir. Bu metodoloji, uluslararası standartlar ve en iyi uygulamalar çerçevesinde yapılandırılmış olup, kuruluşun siber dayanıklılığını artırmak için sistematik bir yaklaşım benimser.

İlk aşamada, kuruluşun mevcut güvenlik durumu detaylı bir şekilde analiz edilir. Bu analiz, varlık envanterinin çıkarılması, güvenlik politikalarının incelenmesi, güvenlik kontrollerinin etkinliğinin değerlendirilmesi ve risk faktörlerinin belirlenmesini kapsar. Kullanılan siber güvenlik teknolojileri, ağ altyapısı, veri koruma mekanizmaları, erişim yönetimi süreçleri ve olay müdahale yetkinlikleri gözden geçirilerek kuruluşun tehdit yüzeyi ortaya konur. Aynı zamanda, tehdit modelleme çalışmaları ile organizasyona yönelik potansiyel saldırı vektörleri ve tehdit aktörleri analiz edilir.

İkinci aşamada, risk değerlendirme süreçleri uygulanarak mevcut tehditlerin iş sürekliliğine, veri gizliliğine ve sistem güvenliğine etkileri ölçümlenir. Bu süreç, olasılık-etki matrisleri, risk skorlamaları ve önceliklendirme yöntemleri ile desteklenerek kritik güvenlik açıklarının belirlenmesini sağlar. Organizasyonun yasal ve regülasyon gereklilikleri çerçevesinde değerlendirilmesi yapılır ve ISO 27001, NIST CSF, CIS Controls, KVKK ve sektörel güvenlik standartlarına uyumluluk seviyeleri analiz edilir.

Üçüncü aşamada, tespit edilen güvenlik açıklarının giderilmesine yönelik stratejik bir yol haritası oluşturulur. Risk azaltma önlemleri belirlenerek kuruluşun siber güvenlik olgunluğunu artıracak teknik, organizasyonel ve operasyonel aksiyon planları geliştirilir. Bu kapsamda, güvenlik sıkılaştırma politikaları, olay müdahale süreçlerinin güçlendirilmesi, güvenlik farkındalık eğitimleri ve sürekli izleme mekanizmaları gibi uygulamalar hayata geçirilir.

Son aşamada ise, geliştirilen güvenlik stratejilerinin etkinliği düzenli olarak ölçülerek süreçlerin sürekli iyileştirilmesi sağlanır. Sürekli izleme, siber tehdit istihbaratı entegrasyonu ve güvenlik testleri aracılığıyla risk yönetim süreçleri güncellenir. Kuruluşun siber güvenlik olgunluğu belirli periyotlarla yeniden değerlendirilerek, dinamik tehdit ortamına uyum sağlayacak şekilde güvenlik politikaları güncellenir.

Bu metodoloji, kuruluşların siber güvenlik stratejilerini güçlendirmesine, riskleri minimize etmesine ve sürdürülebilir bir güvenlik yönetim süreci oluşturmasına olanak tanır.

Mevcut Durum Analizi

Mevcut Durum Analizi kapsamında, kuruluşun mevcut güvenlik altyapısı, politikaları ve süreçleri detaylı bir şekilde incelenerek organizasyonun güvenlik olgunluk seviyesi belirlenir. İlk olarak, kullanılan güvenlik teknolojileri, ağ yapısı, erişim yönetimi, veri koruma yöntemleri ve olay müdahale süreçleri detaylı bir şekilde analiz edilir. Kuruluşun siber tehditlere karşı ne ölçüde dayanıklı olduğu, mevcut güvenlik mekanizmalarının etkinliği ve olası güvenlik açıkları tespit edilir. Bu analiz sürecinde, sistemlerin güvenlik konfigürasyonları, açık portlar, gereksiz servisler, yetkilendirme mekanizmaları ve güvenlik yamalarının güncellik durumu gibi kritik unsurlar değerlendirilir.

Ayrıca, tehdit modelleme çalışmaları ile organizasyona yönelik potansiyel saldırı vektörleri ve tehdit aktörleri belirlenerek olası siber tehdit senaryoları oluşturulur. Organizasyonun geçmişte karşılaştığı siber saldırılar, güvenlik ihlalleri ve olay müdahale kayıtları incelenerek sistemlerin mevcut saldırılara karşı direnci ölçümlenir. Bunun yanı sıra, düzenleyici gereklilikler ve sektör standartları çerçevesinde organizasyonun güvenlik politikaları değerlendirilir ve yürürlükte olan regülasyonlara uyumluluk seviyeleri gözden geçirilir. ISO 27001, NIST CSF, CIS Controls, KVKK, GDPR gibi uluslararası ve yerel standartlara uygunluk derecesi analiz edilerek eksiklikler belirlenir.

Bu kapsamlı analiz süreci sonucunda, kuruluşun tehdit yüzeyi net bir şekilde ortaya konarak güvenlik açıklarının giderilmesi için atılması gereken adımlar belirlenir. Böylece, organizasyonun mevcut güvenlik durumu hakkında detaylı bir görünüm elde edilerek, riskleri minimize etmek ve güvenlik seviyesini artırmak için stratejik bir yol haritası oluşturulur.

Strateji ve Yol Haritası Belirleme

Değerlendirme sonuçlarına dayanarak, organizasyonun güvenlik stratejisini geliştirmek için kapsamlı ve sürdürülebilir bir yol haritası oluşturulur. Bu süreçte, tespit edilen güvenlik açıkları ve riskler detaylı bir şekilde analiz edilerek önceliklendirilir ve her bir riskin organizasyon üzerindeki potansiyel etkisi belirlenir. Kritik güvenlik açıklarının giderilmesine yönelik teknik, operasyonel ve organizasyonel önlemler belirlenirken, kurumun mevcut güvenlik yapısıyla uyumlu olacak şekilde güvenlik sıkılaştırma politikaları uygulanır. Bu doğrultuda, güvenlik altyapısının güçlendirilmesi, olay müdahale süreçlerinin optimize edilmesi, siber güvenlik farkındalık eğitimlerinin düzenlenmesi ve sürekli izleme mekanizmalarının hayata geçirilmesi gibi kapsamlı adımlar planlanır. Ayrıca, organizasyonun güvenlik duruşunu güçlendirmek amacıyla tehdit istihbaratı ve güvenlik izleme çözümleriyle entegre bir yapı oluşturularak, olası saldırılara karşı proaktif bir savunma mekanizması geliştirilir. Sürekli iyileştirme prensibi benimsenerek güvenlik süreçleri düzenli olarak gözden geçirilir, gelişen tehdit ortamına uyum sağlamak adına yeni güvenlik önlemleri devreye alınır ve organizasyonun siber dayanıklılığı en üst seviyeye çıkarılır.

Siber Olgunluk ve Risk Değerlendirme Aşamaları

Siber Olgunluk ve Risk Değerlendirme Hizmeti'nin uygulanma süreci, organizasyonun mevcut siber güvenlik seviyesinin analiz edilmesi, risk faktörlerinin belirlenmesi, güvenlik stratejilerinin oluşturulması ve sürekli iyileştirme süreçlerini kapsar. İlk aşamada, organizasyonun BT altyapısı, güvenlik politikaları, erişim kontrolleri ve olay müdahale süreçleri detaylı bir şekilde incelenerek güvenlik olgunluk seviyesi değerlendirilir. Daha sonra, potansiyel tehdit aktörleri, saldırı vektörleri ve mevcut güvenlik açıkları tespit edilerek risk değerlendirme yöntemleri ile etkileri analiz edilir. Bu analiz doğrultusunda, güvenlik açıklarının giderilmesine yönelik stratejik bir yol haritası oluşturulur ve teknik, operasyonel ve organizasyonel önlemler belirlenir. Sürekli izleme, siber tehdit istihbaratı entegrasyonu ve düzenli güvenlik denetimleri sayesinde, organizasyonun siber güvenlik olgunluğu dinamik tehdit ortamına uyum sağlayacak şekilde sürekli olarak geliştirilir.

Raporlama ve İyileştirme

Siber Olgunluk ve Risk Değerlendirme Hizmeti kapsamında gerçekleştirilen analizler ve değerlendirme sonuçları düzenli olarak raporlanır ve ilgili paydaşlarla paylaşılır. Kuruluşun siber güvenlik seviyesini ölçmek amacıyla yapılan testler, tespit edilen güvenlik açıkları, risk analizi bulguları ve önerilen iyileştirme adımları detaylı olarak teknik ve yönetsel raporlar halinde sunulur. Bu raporlar, hem teknik ekiplerin mevcut güvenlik açıklarını gidermesine yardımcı olmak hem de yönetim seviyesinde stratejik kararların alınmasını sağlamak için özel olarak hazırlanır. Risklerin işletmeye olan etkileri değerlendirilerek, önceliklendirilmesi gereken güvenlik önlemleri belirlenir.

Ayrıca, güvenlik iyileştirme süreçlerinin etkinliği düzenli olarak gözden geçirilir ve organizasyonun siber olgunluk seviyesini artırmaya yönelik sürekli iyileştirme döngüsü uygulanır. Güncel tehdit trendleri, sektörel tehdit istihbaratı ve uluslararası güvenlik standartları takip edilerek, güvenlik politikaları ve kontrolleri güncellenir. Bununla birlikte, organizasyon genelinde siber güvenlik farkındalığını artırmak amacıyla periyodik güvenlik denetimleri, çalışan eğitimleri ve bilinçlendirme programları düzenlenerek kurumsal güvenlik kültürü güçlendirilir.

Sıkça Sorulan Sorular (SSS)

Bu hizmet kapsamında hangi analizler gerçekleştirilir?

Mevcut güvenlik altyapısı, siber güvenlik politikaları, ağ güvenliği, erişim yönetimi, olay müdahale süreçleri ve yasal uyumluluk seviyeleri incelenerek detaylı bir risk analizi yapılır. Tehdit modelleme ve siber saldırı vektörleri değerlendirilerek, organizasyonun maruz kalabileceği riskler belirlenir.

Siber olgunluk seviyesi nasıl belirlenir?

Siber olgunluk seviyesi, uluslararası güvenlik standartları (NIST, ISO 27001, CIS Controls vb.) ve en iyi uygulamalar çerçevesinde belirlenen kriterlere göre değerlendirilir. Organizasyonun mevcut güvenlik kontrolleri, olay yönetim süreçleri ve tehdit istihbaratına dayalı savunma mekanizmaları analiz edilerek seviyelendirilir.

Hangi sektörler için uygundur?

Siber Olgunluk ve Risk Değerlendirme Hizmeti, finans, sağlık, telekomünikasyon, enerji, üretim, kamu ve diğer tüm sektörlerde faaliyet gösteren kuruluşlar için uygundur. Özellikle regülasyonlara tabi sektörlerde, yasal uyumluluğun sağlanmasına da katkıda bulunur.

Hizmetin organizasyona sağladığı faydalar nelerdir?

Bu hizmet, kuruluşların siber güvenlik stratejilerini güçlendirmesine, güvenlik açıklarını gidermesine ve olası saldırılara karşı daha dirençli hale gelmesine yardımcı olur. Riskleri minimize ederek, güvenlik olaylarının iş sürekliliğine etkisini azaltır ve yasal uyumluluk süreçlerini kolaylaştırır.

Hizmet kapsamında hangi standartlar ve metodolojiler kullanılır?

Hizmet, NIST Cybersecurity Framework, ISO 27001, CIS Controls, MITRE ATT&CK ve diğer uluslararası güvenlik standartları temel alınarak yürütülür. Risk değerlendirme süreçlerinde endüstri en iyi uygulamaları ve güncel tehdit istihbaratı da kullanılır.

Bu hizmet düzenli olarak alınmalı mı?

Evet. Siber tehditler sürekli geliştiği için, organizasyonların güvenlik seviyelerini düzenli olarak değerlendirmesi ve risk analizlerini güncellemesi önemlidir. Özellikle yeni teknolojilerin entegrasyonu, büyük altyapı değişiklikleri veya güvenlik ihlalleri sonrası bu hizmetin tekrarlanması önerilir.