EMA SECURITY

vCISO 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

vCISO (Sanal Bilgi Güvenliği Yöneticisi) Hizmeti, kuruluşların siber güvenlik stratejilerini yönetmek, riskleri minimize etmek ve yasal uyumluluğu sağlamak amacıyla deneyimli bir güvenlik yöneticisi desteği almasını sağlayan esnek ve kapsamlı bir güvenlik çözümüdür. Günümüzde artan siber tehditler ve regülasyon baskıları, organizasyonların güvenlik yönetimini profesyonel bir bakış açısıyla ele almasını zorunlu hale getirmektedir. Ancak, birçok kuruluş için tam zamanlı bir CISO (Chief Information Security Officer) istihdam etmek maliyetli ve operasyonel olarak zorlayıcı olabilir. vCISO hizmeti, bu ihtiyaca yönelik olarak uzman bir güvenlik liderinin organizasyona danışmanlık yapmasını ve siber güvenlik süreçlerini etkin bir şekilde yönetmesini sağlar.

Bu hizmet kapsamında, kuruluşun mevcut siber güvenlik durumu detaylı bir şekilde analiz edilir ve organizasyona özel güvenlik stratejileri geliştirilir. ISO 27001, NIST Cybersecurity Framework, CIS Controls, GDPR, KVKK gibi uluslararası standartlar ve regülasyonlar temel alınarak güvenlik politikaları oluşturulur ve organizasyonun uyumluluk seviyeleri değerlendirilir. vCISO, tehdit yönetimi, risk analizi, güvenlik mimarisi tasarımı, olay müdahale planları ve kriz yönetimi gibi kritik süreçleri yöneterek organizasyonun güvenlik olgunluğunu artırır.

Ayrıca, kuruluşun güvenlik açıklarını belirlemek, riskleri önceliklendirmek ve uygun siber güvenlik kontrollerini uygulamak için düzenli denetimler gerçekleştirilir. vCISO, güvenlik farkındalığı eğitimleri düzenleyerek çalışanların bilinç seviyesini artırırken, güvenlik süreçlerinin operasyonel süreçlere entegrasyonunu sağlar. Aynı zamanda, tehdit istihbaratı desteği sunarak gelişen tehdit ortamına karşı organizasyonun proaktif bir güvenlik yaklaşımı benimsemesini sağlar.

vCISO hizmeti, BT ve güvenlik ekipleriyle koordineli bir şekilde çalışarak organizasyonun siber güvenlik yönetimini sürekli geliştirir ve saldırı yüzeyini en aza indirir. Bu sayede, kuruluşlar yüksek maliyetli bir tam zamanlı CISO pozisyonuna ihtiyaç duymadan uzman bir güvenlik yöneticisinin deneyiminden faydalanabilirler. Stratejik güvenlik yönetimi, kriz anlarında liderlik ve uzun vadeli güvenlik planlaması gibi kritik yetkinlikleri organizasyona kazandırarak, vCISO hizmeti kuruluşların siber dayanıklılığını artıran değerli bir çözüm sunar.

Hizmete Ait Bileşenler

Siber Güvenlik Stratejisi ve Yol Haritası Geliştirme

Kuruluşun mevcut güvenlik durumu detaylı bir şekilde analiz edilerek, organizasyonun ihtiyaçlarına uygun stratejik bir yol haritası oluşturulur. Bu süreçte, kısa, orta ve uzun vadeli güvenlik hedefleri belirlenir, önceliklendirilir ve uygulanacak güvenlik politikaları tanımlanarak organizasyonun güvenlik olgunluğu artırılır.

Risk Değerlendirme ve Yönetimi

Organizasyonun varlıkları, tehditler ve mevcut güvenlik açıkları analiz edilerek kapsamlı bir risk değerlendirmesi gerçekleştirilir. Risklerin iş süreçlerine etkisi ölçümlenir, olasılık ve etki bazlı önceliklendirme yapılır ve güvenlik açıklarını gidermeye yönelik uygun kontroller planlanarak etkin bir risk yönetim süreci oluşturulur.

Uyumluluk ve Regülasyon Yönetimi

ISO 27001, NIST CSF, GDPR, KVKK, PCI-DSS gibi uluslararası ve sektörel regülasyonlar doğrultusunda organizasyonun mevcut uyumluluk seviyesi değerlendirilir. Güvenlik politikaları ve prosedürler, yasal ve düzenleyici gerekliliklere uygun şekilde geliştirilerek, organizasyonun siber güvenlik ve veri koruma yükümlülüklerini eksiksiz yerine getirmesi sağlanır.

Olay Müdahale ve Kriz Yönetimi

Siber saldırılar ve güvenlik olayları karşısında hızlı ve etkili müdahale sağlamak amacıyla olay yönetimi süreçleri oluşturulur. Güvenlik ihlallerine karşı kriz yönetim planları hazırlanır, tatbikatlar düzenlenerek ekiplerin olaylara karşı hazırlık seviyeleri artırılır ve olay sonrası iyileştirme süreçleri etkin şekilde yönetilir.

Tehdit İstihbaratı ve Güvenlik İzleme

Güncel tehditler, saldırı yöntemleri ve siber saldırganların stratejileri takip edilerek organizasyonun proaktif güvenlik önlemleri alması sağlanır. SIEM, EDR ve XDR gibi güvenlik çözümleri ile entegre edilen izleme mekanizmaları sayesinde anormal aktiviteler tespit edilir ve güvenlik olaylarına erken müdahale edilerek riskler minimize edilir.

Güvenlik Politikaları ve Prosedürlerinin Geliştirilmesi

Organizasyonun iş süreçleri, teknoloji altyapısı ve operasyonel gereksinimleri göz önünde bulundurularak kapsamlı güvenlik politikaları ve prosedürler oluşturulur. Bu süreçte, erişim yönetimi, veri koruma, kimlik doğrulama, olay müdahale ve güvenlik yönetimi gibi alanlar için en iyi uygulamalar belirlenerek güvenlik çerçevesi güçlendirilir.

Siber Güvenlik Farkındalık ve Eğitim Programları

Çalışanların sosyal mühendislik saldırıları, kimlik avı tehditleri ve siber güvenlik farkındalığı konularında bilinçlenmesini sağlamak amacıyla düzenli eğitim programları ve tatbikatlar gerçekleştirilir. Üst yönetim ve teknik ekipler için özel eğitim oturumları düzenlenerek organizasyon genelinde güçlü bir siber güvenlik kültürü oluşturulur.

Tedarikçi ve Üçüncü Taraf Güvenlik Değerlendirmesi

Organizasyonun iş birliği yaptığı üçüncü taraf tedarikçilerin ve hizmet sağlayıcılarının güvenlik seviyeleri değerlendirilerek, tedarik zinciri kaynaklı riskler analiz edilir. Güvenlik açıklarını en aza indirmek için güvenlik kontrolleri belirlenir, sözleşmelerde güvenlik gereklilikleri tanımlanır ve düzenli denetimler gerçekleştirilerek üçüncü taraf risk yönetimi süreçleri uygulanır.

BT ve Güvenlik Ekipleri ile Koordinasyon

BT ve güvenlik ekipleriyle yakın iş birliği içinde çalışarak organizasyonun güvenlik süreçleri optimize edilir, güvenlik kontrollerinin etkin uygulanması sağlanır ve yeni güvenlik çözümlerinin entegrasyonu konusunda danışmanlık verilir. Bu süreçte, teknik ekiplerin güncel güvenlik tehditleri ve en iyi uygulamalar konusunda bilinçlendirilmesi sağlanarak organizasyonun genel güvenlik seviyesi yükseltilir.

Sürekli Güvenlik İyileştirme ve Raporlama

Organizasyonun siber güvenlik durumu periyodik olarak değerlendirilerek güvenlik açıkları ve iyileştirme alanları belirlenir. Yönetim ve teknik ekipler için kapsamlı güvenlik raporları hazırlanarak mevcut riskler, tehditler ve alınması gereken önlemler hakkında bilgilendirme yapılır. Sürekli iyileştirme prensibi doğrultusunda güvenlik stratejileri dinamik tehdit ortamına uyum sağlayacak şekilde güncellenir.

Siber Olgunluk ve Risk Değerlendirme Metodolojisi

vCISO Hizmeti, kuruluşların siber güvenlik yönetim süreçlerini güçlendirmek, riskleri etkin bir şekilde yönetmek ve güvenlik stratejilerini geliştirmek amacıyla sunulan kapsamlı bir danışmanlık hizmetidir. Bu metodoloji, uluslararası siber güvenlik standartlarına ve en iyi uygulamalara dayalı olarak yapılandırılmış olup, kuruluşların güvenlik olgunluk seviyelerini artırmaya yönelik stratejik ve operasyonel bir yaklaşım benimser.

İlk aşamada, organizasyonun mevcut siber güvenlik durumu analiz edilir ve güvenlik olgunluğu değerlendirilir. Bu süreçte, mevcut güvenlik politikaları, kontroller, risk yönetim süreçleri, tehdit istihbaratı kullanımı, olay müdahale planları ve regülasyon uyumluluğu gibi unsurlar detaylı olarak incelenir. Aynı zamanda, siber tehdit yüzeyi belirlenerek organizasyonun maruz kalabileceği riskler ve saldırı vektörleri analiz edilir. İş süreçlerine entegre olan dijital varlıklar, kritik sistemler ve veri koruma mekanizmaları değerlendirilerek, güvenlik açıkları ve iyileştirme alanları tespit edilir.

İkinci aşamada, organizasyonun risk yönetim süreçleri güçlendirilir ve güvenlik stratejileri oluşturulur. ISO 27001, NIST CSF, CIS Controls, PCI-DSS, GDPR, KVKK gibi uluslararası ve sektörel standartlar doğrultusunda güvenlik politikaları yeniden yapılandırılır ve uyumluluk süreçleri optimize edilir. Bu kapsamda, güvenlik riskleri değerlendirilir, olasılık-etki analizleri yapılır ve kuruluşun operasyonel gereksinimlerine uygun bir risk yönetim çerçevesi oluşturulur. Tehdit istihbaratı sistemleri, güvenlik izleme çözümleri ve olay yönetim süreçleri entegre edilerek organizasyonun proaktif tehdit tespit yetkinliği artırılır.

Üçüncü aşamada, siber güvenlik stratejilerinin etkinliğini artırmak amacıyla teknik ve organizasyonel önlemler uygulanır. Kimlik ve erişim yönetimi, güvenlik sıkılaştırma politikaları, olay müdahale planları, veri koruma stratejileri ve güvenlik farkındalık eğitimleri hayata geçirilerek kuruluş genelinde güçlü bir güvenlik kültürü oluşturulur. Siber güvenlik operasyonlarının sürekli iyileştirilmesini sağlamak amacıyla güvenlik denetimleri gerçekleştirilir ve organizasyonun tehdit ortamına uyum sağlaması için düzenli değerlendirmeler yapılır.

Son aşamada, vCISO hizmeti kapsamında oluşturulan güvenlik stratejileri sürekli olarak izlenir, değerlendirilir ve iyileştirilir. Siber güvenlik performans metrikleri ve düzenli güvenlik raporları aracılığıyla yönetim seviyesinde bilgilendirme sağlanır ve organizasyonun güvenlik duruşu periyodik olarak gözden geçirilir. Olay yönetim süreçleri, kriz müdahale planları ve tehdit istihbaratı entegrasyonu gibi unsurlar dinamik tehdit ortamına uyum sağlayacak şekilde güncellenerek kuruluşun siber dirençliliği artırılır.

Bu metodoloji, kuruluşların güvenlik risklerini etkin bir şekilde yönetmesine, siber güvenlik süreçlerini optimize etmesine ve operasyonel sürekliliğini korumasına yardımcı olarak güçlü ve sürdürülebilir bir güvenlik yönetim çerçevesi oluşturmasına olanak tanır.

Mevcut Durum Analizi

vCISO Hizmeti kapsamında, kuruluşun mevcut siber güvenlik durumu kapsamlı bir şekilde analiz edilerek güvenlik olgunluk seviyesi belirlenir. İlk olarak, organizasyonun güvenlik stratejisi, politikaları, süreçleri ve teknolojik altyapısı değerlendirilerek güçlü ve zayıf yönler tespit edilir. Kullanılan güvenlik teknolojileri, erişim yönetimi, veri koruma yöntemleri ve olay müdahale süreçleri incelenerek tehdit modelleme çalışmalarıyla potansiyel saldırı vektörleri belirlenir.

Bu süreçte, geçmiş güvenlik ihlalleri ve olay müdahale kayıtları analiz edilerek sistemlerin mevcut tehditlere karşı direnci ölçümlenir. Sistem konfigürasyonları, yetkilendirme mekanizmaları ve güvenlik güncellemeleri gözden geçirilerek kritik açıklar tespit edilir. Ayrıca, ISO 27001, NIST CSF, CIS Controls, KVKK ve GDPR gibi regülasyonlara uyumluluk değerlendirilerek eksiklikler belirlenir.

Analiz sonucunda, organizasyonun tehdit yüzeyi net bir şekilde ortaya konarak güvenlik risklerini azaltmak için stratejik bir yol haritası oluşturulur. vCISO, güvenlik politikalarını optimize edip operasyonel güvenliği sürdürülebilir hale getirerek organizasyonun tehditlere karşı proaktif bir güvenlik yaklaşımı kazanmasını sağlar.

Strateji ve Yol Haritası Belirleme

vCISO Hizmeti kapsamında, kuruluşun siber güvenlik stratejisini geliştirmek ve uzun vadeli güvenlik hedeflerine ulaşmasını sağlamak amacıyla kapsamlı bir yol haritası oluşturulur. Değerlendirme sonuçlarına dayanarak, mevcut güvenlik açıkları ve riskler analiz edilerek önceliklendirilir, her riskin organizasyon üzerindeki etkisi belirlenir ve kritik güvenlik açıklarının giderilmesine yönelik stratejik adımlar planlanır. Bu süreçte, güvenlik politikalarının güçlendirilmesi, olay müdahale süreçlerinin optimize edilmesi, güvenlik farkındalık eğitimlerinin artırılması ve sürekli izleme mekanizmalarının hayata geçirilmesi gibi önlemler devreye alınır. Kurumun siber tehditlere karşı proaktif bir savunma yaklaşımı benimsemesi için tehdit istihbaratı ve güvenlik izleme çözümleri entegre edilerek, saldırılara karşı dinamik bir güvenlik yapısı oluşturulur. Sürekli iyileştirme prensibi doğrultusunda güvenlik süreçleri düzenli olarak gözden geçirilir, gelişen tehdit ortamına uyum sağlamak için yeni güvenlik önlemleri uygulanır ve organizasyonun siber dayanıklılığı en üst seviyeye çıkarılır. vCISO, yönetim katmanıyla iş birliği içinde çalışarak güvenlik stratejilerinin iş hedefleriyle uyumlu hale getirilmesini sağlar ve organizasyonun siber güvenlik olgunluğunu sürdürülebilir bir şekilde artırır.

vCISO Hizmet Aşamaları

vCISO Hizmeti, organizasyonun mevcut güvenlik seviyesinin analiz edilmesi, risklerin belirlenmesi ve güvenlik stratejilerinin oluşturulmasını kapsar. İlk olarak, BT altyapısı, erişim kontrolleri ve olay müdahale süreçleri değerlendirilerek güvenlik olgunluğu belirlenir. Ardından, tehdit aktörleri ve güvenlik açıkları analiz edilerek risk yönetim stratejileri geliştirilir. Bu doğrultuda, güvenlik mimarisi güçlendirilir, olay müdahale süreçleri iyileştirilir ve farkındalık eğitimleri düzenlenir. Sürekli izleme ve tehdit istihbaratı entegrasyonu ile organizasyonun güvenlik seviyesi dinamik tehdit ortamına uyum sağlayacak şekilde geliştirilmeye devam edilir.

Raporlama ve İyileştirme

vCISO Hizmeti kapsamında gerçekleştirilen analizler ve değerlendirme sonuçları düzenli olarak raporlanarak ilgili paydaşlarla paylaşılır. Yapılan güvenlik testleri, tespit edilen güvenlik açıkları, risk analizleri ve önerilen iyileştirme adımları teknik ve yönetsel raporlar halinde sunulur. Bu raporlar, teknik ekiplerin güvenlik açıklarını gidermesine yardımcı olurken, yönetim seviyesinde stratejik kararların alınmasını da destekler. Risklerin işletmeye etkileri değerlendirilerek önceliklendirilmesi gereken güvenlik önlemleri belirlenir. Ayrıca, sürekli iyileştirme kapsamında, tehdit istihbaratı ve güncel güvenlik trendleri takip edilerek güvenlik politikaları güncellenir. Periyodik güvenlik denetimleri, çalışan eğitimleri ve bilinçlendirme programları ile organizasyon genelinde siber güvenlik farkındalığı artırılarak 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.