EMA SECURITY

Siber Olay Müdahale 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 Olay Müdahalesi Hizmeti, organizasyonların siber tehditlere karşı etkin bir şekilde yanıt vermelerini sağlayan kapsamlı bir süreçtir. Günümüzde siber saldırılar giderek karmaşık hale gelmekte ve organizasyonlar için ciddi operasyonel ve finansal riskler oluşturmaktadır. Bu hizmetin temel amacı, güvenlik ihlallerini hızlı bir şekilde tespit etmek, etkilerini minimize etmek ve olay sonrası iyileştirme süreçlerini etkin bir şekilde yönetmektir. ISO 27035, NIST 800-61 ve diğer uluslararası güvenlik standartlarına dayanan bu süreç; olay tespiti, analiz, müdahale, iyileştirme ve sürekli izleme aşamalarını içerir.

Siber olay yönetimi sürecinde, saldırı vektörleri analiz edilerek güvenlik olaylarının kaynağı tespit edilir ve tehdit aktörlerinin izleri takip edilir. Olay müdahale ekipleri, güvenlik açıklarını belirleyerek tehditlerin yayılmasını önlemek için hızlı aksiyonlar alır. Olayın etkileri değerlendirilerek, sistemlerin normal operasyonlarına dönmesini sağlayacak adımlar belirlenir. Ayrıca, saldırı sonrası adli analiz çalışmaları gerçekleştirilerek saldırganın yöntemi ve motivasyonu detaylı bir şekilde incelenir.

Siber olay müdahalesi tek seferlik bir süreç olmayıp, sürekli iyileştirme ve izleme gerektiren dinamik bir yaklaşıma sahiptir. Organizasyonların güvenlik politikaları, olay sonrası analizlerle geliştirilerek gelecekte benzer tehditlere karşı daha dirençli hale getirilir. Aynı zamanda, tehdit istihbaratı sistemleriyle entegrasyon sağlanarak potansiyel tehditler önceden tespit edilir ve riskler minimize edilir.

Siber Olay Müdahalesi Hizmeti, organizasyonların güvenlik olaylarına karşı daha hazırlıklı olmalarına ve saldırılara karşı hızlı, etkin yanıt verebilmelerine olanak tanır. Yönetim ekiplerine sunulan raporlar sayesinde, saldırıların kök nedenleri analiz edilerek güvenlik politikaları güçlendirilir. Bu hizmet, yalnızca mevcut güvenlik olaylarını yönetmekle kalmaz, aynı zamanda organizasyonun uzun vadeli güvenlik duruşunu güçlendirmeye yardımcı olur.

Siber Olay Müdahalesi Metodolojisi

Siber Olay Müdahalesi süreci, organizasyonların siber tehditlere karşı hızlı ve etkili bir şekilde yanıt verebilmesini sağlamak amacıyla belirli metodolojik yaklaşımlar doğrultusunda yürütülmektedir. Bu süreç, olayın başarılı bir şekilde yönetilmesini ve gelecekte benzer saldırıların önlenmesini sağlamak için birden fazla aşamadan oluşur.

Hazırlık aşamasında, organizasyonun güvenlik politikaları ve olay müdahale prosedürleri belirlenir. Olay müdahale ekipleri oluşturularak görev dağılımları yapılır ve personelin gerekli teknik eğitimleri alması sağlanır. Güvenlik olaylarına karşı etkili bir müdahale yapabilmek için tehdit istihbaratı sistemleri entegre edilir ve simülasyonlar gerçekleştirilerek organizasyonun olaylara karşı hazırlık seviyesi test edilir. Bu aşamada ayrıca olay yönetim süreçlerini hızlandırmak için otomatik izleme ve uyarı sistemleri kurulur.

Tanımlama aşamasında, güvenlik olaylarının tespiti yapılır ve olayın kapsamı belirlenir. Güvenlik izleme sistemlerinden gelen alarmlar analiz edilerek saldırının kaynağı, hedefi ve saldırganın yöntemleri tespit edilmeye çalışılır. Bu aşamada olayın yanlış pozitif olup olmadığı değerlendirilir ve saldırının sistemlere etkisi belirlenerek acil aksiyon planları hazırlanır.

İçerme (containment) aşamasında, olayın daha fazla yayılmasını önlemek için hızlı önlemler alınır. Etkilenen sistemlerin izole edilmesi, belirli ağ segmentlerinin geçici olarak devre dışı bırakılması veya saldırganın erişim yollarının kesilmesi gibi aksiyonlar uygulanır. Organizasyonun iş sürekliliğini sağlamak için kritik sistemler koruma altına alınır ve mümkünse saldırganın daha fazla zarar vermesi engellenir.

Ortadan kaldırma (eradication) sürecinde, saldırının kaynağı sistemlerden tamamen temizlenir. Kötü amaçlı yazılımlar kaldırılır, saldırıya neden olan güvenlik açıkları kapatılır ve ilgili sistemlerde gerekli güncellemeler yapılır. Siber olayın tekrar yaşanmaması için yeni güvenlik kontrolleri uygulanır ve sistemler detaylı bir güvenlik taramasından geçirilir.

Kurtarma (recovery) aşamasında, saldırıdan etkilenen sistemlerin güvenli bir şekilde tekrar çalışır hale getirilmesi sağlanır. Geri yükleme işlemleri gerçekleştirilirken, sistemlerin güvenli bir durumda olduğundan emin olunması için detaylı testler yapılır. Olayın tamamen sona erdiği doğrulandıktan sonra, operasyonlar normal akışına döndürülür.

Öğrenme ve geliştirme aşamasında, olay sonrası detaylı analizler gerçekleştirilerek süreç boyunca alınan dersler değerlendirilir. Olayın nedenleri, saldırı yöntemleri ve güvenlik açıkları belirlenerek organizasyon için geliştirilecek güvenlik önlemleri tespit edilir. Bu bilgiler ışığında güvenlik politikaları güncellenir, çalışanlara yönelik bilinçlendirme eğitimleri düzenlenir ve organizasyonun genel güvenlik duruşunu güçlendirecek aksiyonlar belirlenir. Tehdit istihbaratı sistemleriyle entegrasyon sağlanarak, gelecekte benzer olayların daha erken tespit edilmesi ve önlenmesi için proaktif güvenlik stratejileri uygulanır.

Hizmete Ait Bileşenler

Olay İzleme ve Tespit

Olay izleme ve tespit sürecinde, güvenlik olaylarının anlık olarak izlenmesi ve anormal aktivitelerin tespit edilmesi sağlanır. Sistemlerden gelen log kayıtları, ağ trafiği ve uç nokta verileri sürekli analiz edilerek anomali tespiti gerçekleştirilir. SIEM (Security Information and Event Management) sistemleri kullanılarak anlık tehditler belirlenir ve olay müdahale süreci başlatılır.

Acil Durum Müdahale Planı

Önceden belirlenmiş prosedürler doğrultusunda, olaylara hızlı ve etkili müdahale edilmesi hedeflenir. Organizasyon içindeki sorumlu ekipler belirlenir, olay esnasında hangi adımların uygulanacağı tanımlanır ve acil durum senaryoları oluşturulur. Etkin bir müdahale planı, olayın etkisini en aza indirerek iş sürekliliğini sağlamaya yardımcı olur.

Tehdit Analizi ve Değerlendirme

Saldırının kaynağı, yöntemi ve etkileri detaylı olarak analiz edilir. Tehdit aktörlerinin kimlikleri, motivasyonları ve teknikleri araştırılır. Bu analiz sonucunda organizasyonun güvenlik açıkları tespit edilerek gelecekte benzer tehditlerin önlenmesine yönelik stratejiler oluşturulur.

İzolasyon ve Etki Azaltma

Güvenliği ihlal edilen sistemler izole edilerek zararın en aza indirilmesi sağlanır. Bu süreç, saldırının organizasyon geneline yayılmasını önlemek ve etkilenen sistemlerin hızla kontrol altına alınmasını sağlamak amacıyla uygulanır.

Olay Sonrası İyileştirme

Güvenlik zafiyetleri kapatılarak sistemler güçlendirilir ve gelecekte benzer saldırılara karşı koruma sağlanır. Organizasyonların güvenlik politikaları güncellenerek risk yönetim stratejileri geliştirilir ve olası tehditlere karşı daha dirençli hale gelinmesi sağlanır.

Adli Bilişim Analizi

Saldırganın kimliği, motivasyonu ve teknikleri hakkında bilgi toplanır ve kanıtların saklanması sağlanır. Dijital izler takip edilerek olayın tam olarak nasıl gerçekleştiği ortaya konur ve hukuki süreçlere destek sağlanır.

Raporlama ve Sürekli İyileştirme

Müdahale süreci dökümante edilerek organizasyonun güvenlik politikaları sürekli olarak geliştirilir. Olay sonrası analizlerden elde edilen veriler ışığında yeni güvenlik önlemleri belirlenir ve gelecekteki tehditlere karşı daha hazırlıklı olunması sağlanır.

Mevcut Durum Analizi

Siber Olay Müdahalesi Hizmeti öncesinde, kuruluşun güvenlik altyapısı, olay izleme sistemleri ve tehdit algılama mekanizmaları değerlendirilerek müdahale kapasitesi belirlenir. Olası güvenlik açıkları, tehdit vektörleri ve geçmiş siber olaylar analiz edilerek organizasyonun saldırılara karşı dayanıklılığı ölçümlenir.

Ayrıca, Dark Web ve siber suç platformlarında kuruluş hakkında sızdırılmış veriler araştırılır. Sektöre özgü tehditler ve olası saldırı senaryoları belirlenerek, tehdit istihbaratı ile entegre bir olay müdahale stratejisi oluşturulur. Bu sayede, hızlı ve etkili müdahale süreçleri geliştirilerek kuruluşun siber dayanıklılığı artırılır.

Strateji ve Yol Haritası Belirleme

Siber Olay Müdahalesi Hizmeti'nin etkin bir şekilde uygulanabilmesi için kapsamlı bir strateji ve yol haritası oluşturulur. Olay müdahale süreçlerinin operasyonel, taktiksel ve stratejik seviyelerde nasıl yönetileceği planlanır. SIEM, SOAR ve EDR gibi güvenlik çözümleriyle entegrasyon sağlanarak olay tespiti ve müdahale süreçleri hızlandırılır.

Siber Olay Müdahalesi Aşamaları

Siber Olay Müdahalesi Hizmeti kapsamında tehdit istihbaratı, olaylara hızlı yanıt verebilmek için güvenlik sistemlerine entegre edilir. İlk aşamada, farklı kaynaklardan tehdit verileri toplanarak analiz edilir ve tespit edilen tehdit göstergeleri (IOC) ile saldırı teknikleri (TTP) belirlenir.

Bu veriler, SIEM, SOAR ve EDR gibi sistemlerle entegre edilerek olay tespit ve müdahale süreçleri güçlendirilir. Tehdit istihbaratı sayesinde saldırılar hızla tespit edilip etkileri en aza indirilir. Sürekli izleme ve güncelleme süreçleriyle organizasyonun siber tehditlere karşı dayanıklılığı artırılır.

Raporlama ve İyileştirme

Siber Olay Müdahalesi Hizmeti kapsamında elde edilen tehdit istihbaratı verileri düzenli olarak raporlanır ve analiz edilir. Tespit edilen saldırılar, olay müdahale süreçleri ve alınan önlemler detaylandırılarak teknik ekipler ve yönetim için ayrı formatlarda sunulur.

Müdahale süreçlerinin etkinliği değerlendirilerek güvenlik politikaları sürekli iyileştirilir. Güncel tehdit trendleri takip edilerek kuruluşun savunma mekanizmaları güçlendirilir. Ayrıca, olaylara daha hızlı ve etkili yanıt verebilmek amacıyla düzenli eğitimler ve tatbikatlar gerçekleştirilir.

Sıkça Sorulan Sorular (SSS)

Siber Olay Müdahalesi Hizmeti neden gereklidir?

Siber tehditler sürekli gelişmekte ve organizasyonlar için büyük risk oluşturmaktadır. Güvenlik ihlallerine hızlı ve etkin müdahale edilmezse, veri kaybı, finansal zararlar ve itibar kaybı gibi ciddi sonuçlar doğabilir.

Hangi tür siber olaylara müdahale edilir?

Hizmet; kötü amaçlı yazılım saldırıları, fidye yazılımları, veri ihlalleri, DDoS saldırıları, kimlik avı saldırıları, içeriden tehditler ve gelişmiş kalıcı tehditler (APT) gibi geniş bir saldırı yelpazesine müdahale eder.

Olay müdahalesi sırasında organizasyonun operasyonları kesintiye uğrar mı?

Belirli operasyonel kesintiler yaşanabilir, ancak sürecin hızlı ve etkili yürütülmesiyle bu kesintiler en aza indirilir.

Olay müdahale süreci ne kadar sürer?

Olayın ciddiyetine bağlı olarak birkaç saatten birkaç haftaya kadar sürebilir.

Siber olaylara karşı nasıl daha iyi hazırlanılabilir?

Düzenli sızma testleri, güvenlik farkındalık eğitimleri ve güçlü güvenlik politikaları uygulanarak organizasyonlar daha dirençli hale gelebilir.

Olay müdahalesi sürecinde hangi araçlar kullanılır?

Olay yönetimi için SIEM (Security Information and Event Management) sistemleri, tehdit istihbaratı platformları, adli bilişim yazılımları, uç nokta tespit ve müdahale (EDR) araçları gibi çeşitli güvenlik teknolojileri kullanılır.

Olay sonrası organizasyonun güvenliği nasıl artırılır?

Saldırıya neden olan güvenlik açıkları kapatılarak sistemler güçlendirilir. Ayrıca, olay sonrası raporlar hazırlanarak güvenlik önlemleri sürekli olarak güncellenir ve geliştirilir.

Siber olay müdahalesi ile sigorta hizmetleri nasıl entegre edilebilir?

Siber güvenlik sigortaları, olay müdahalesi süreçleri ile uyumlu hale getirilerek finansal risklerin azaltılmasını sağlar. Kuruluşlar, olay sonrası tazminatlar ve mali kayıpların telafi edilmesi için sigorta sağlayıcıları ile entegre çalışabilir.