Privia SECURITY

Olay Müdahale Hizmeti

Profesyonel Defensive Security Hizmetleri

"Siber Olaylara Anında Müdahale!"

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

+90 (216) 514 72 14

www.priviasecurity.com

“Siber olaylara anlık müdahale, tehditlerin hızlıca kontrol altına alınmasını ve güvenliğin tekrar normale dönmesini sağlar.”

Olay Müdahale Hizmeti, organizasyonların karşılaşabileceği siber saldırılara ve güvenlik ihlallerine hızlı bir yanıt verebilmesi için tasarlanmış kapsamlı bir güvenlik hizmetidir. Siber tehditlerin hızla değişen doğası göz önüne alındığında, etkin bir olay müdahalesi, organizasyonun iş sürekliliğini korumada kritik bir rol oynar. Güvenlik ihlalleri sırasında, olayın boyutuna göre en uygun müdahale stratejisi belirlenir ve uygulanır.

Olay müdahalesi sürecinde, tehditleri tespit etmek ve etkili bir şekilde izole etmek öncelikli hedefler arasındadır. Güvenlik ekibi, tespit edilen tehditler doğrultusunda izlenecek adımları belirleyerek hızla harekete geçer. Bu süreçte kullanılan teknolojiler, tehditlerin gerçek zamanlı olarak izlenmesini ve müdahale hızını artırır. Olayın etkilerini minimumda tutmak amacıyla izolasyon adımları devreye alınır.

İç tehditler, çalışan hataları veya kötü niyetli iç saldırganlardan kaynaklanabilirken, dış tehditler siber suçlular veya rakip organizasyonlar tarafından gerçekleştirilebilir. Olay müdahalesi süreci, tüm bu tehdit kaynaklarını kapsayacak şekilde geniş bir perspektifte tasarlanmıştır. Bir güvenlik ihlalinin ardından yapılan adli analizler, olayın nedenini ve saldırının kaynağını belirlemek için detaylı incelemeler içerir. Adli analiz süreci, güvenlik ekibinin saldırının izlerini takip etmesine ve benzer tehditleri önleyici adımlar atılmasına yardımcı olur

Olay Müdahale Hizmeti ayrıca, organizasyonun yasal gereksinimlere uyum sağlamasını destekler. Güvenlik ihlali durumunda düzenleyici kurumlarla iş birliği yapılması ve gerekli raporlamaların sağlanmasını sağlar.

Hizmete Ait Bileşenler

Olay Tespiti ve Analizi

Olay tespiti, siber tehditlerin hızlı bir şekilde tanımlanması ve analiz edilmesi sürecini kapsar. Güvenlik ekibi, izleme araçları aracılığıyla şüpheli etkinlikleri ve olası tehditleri tespit eder. Tehdit tespiti sırasında, saldırının kaynakları, hedeflenen sistemler ve saldırı türü detaylı olarak analiz edilir. Gerçekleştirilen analizler sayesinde saldırının boyutu, etkisi belirlenir ve gerekli müdahale adımları hızlıca devreye alınır. Organizasyon, bu süreçte olayın sebebini daha iyi anlar ve diğer tehditlere karşı hazırlıklı hale gelir.

Tehdit İzolasyonu ve Kontrol

Tehdit izolasyonu, güvenlik ihlallerinin organizasyon genelinde yayılmasını önlemek için tehditlerin izole edilmesi sürecini kapsar. İzolasyon adımları güvenlik ekiplerinin, tehdidin yayıldığı sistemleri hızla kontrol altına almasına olanak tanır. Sistemlerin izole edilmesi, saldırının daha geniş bir alana yayılmasının önüne geçer ve diğer sistemlerin güvenliğine katkı sağlar. Kullanılan araçlar izleme ve izolasyon adımlarının hızlı ve etkili bir şekilde yapılmasını destekler. Tehdit kontrol süreci, organizasyonun güvenlik ihlallerini yönetebilmesi için güvenli bir ortam sunar.

Olay Müdahale Süreci

Olay müdahale süreci, siber güvenlik ekibimizin tehditlere hızlı bir şekilde yanıt vererek olayı kontrol altına almasını kapsar. Güvenlik ihlalleri sırasında, en uygun müdahale adımları belirlenir ve hızla uygulanır. Belirlenen adımlar, olayın türüne ve organizasyonun ihtiyaçlarına göre özelleştirilir. Olay müdahalesi, saldırının neden olduğu zararların en aza indirilmesine yardımcı olur. Siber güvenlik ekiplerimiz, tehditlerin kontrol altına alınmasını sağlayarak, organizasyonun iş sürekliliğini korur.

Adli Analiz ve İz Takibi

Adli analiz süreci, olay sonrası güvenlik ihlalinin nedenlerini belirlemek ve saldırganın izlerini takip etmek için detaylı incelemeler içerir. Siber güvenlik ekiplerimiz, saldırının izlerini takip ederek saldırının hangi sistemler üzerinde nasıl bir etkiye yol açtığını analiz eder. Elde edilen veriler, olay müdahalesinin etkinliğini değerlendirmek için de kullanılır. Saldırganın yöntemlerini anlamak için kritik veriler sunar ve güvenlik altyapısında gerekli iyileştirmelerin yapılmasını sağlar. Elde edilen bulgular, güvenlik politikalarının güncellenmesi için rehberlik eder.

İletişim ve Raporlama

Olay müdahale sürecinde etkili iletişim, kriz anında bilgi akışını sağlayarak sürecin yönetilmesine yardımcı olur. İç ve dış paydaşlarla doğru ve zamanında iletişim, olayın yönetilmesinde kritik rol oynar. Bilgi güvenliği ihlallerinde yönetim, güvenlik ekipleri ve gerekirse düzenleyici kurumlar bilgilendirilir. Olayın etkileri ve alınan önlemler

hakkında detaylı raporlar hazırlanır. Raporlar hem sürecin değerlendirilmesine hem de yasal uyumun sağlanmasına katkı sağlar. İletişim protokolleri, organizasyonun kriz anında hızlı hareket etmesini kolaylaştırır.

Önleyici Tedbirlerin Alınması

Olay müdahale sürecinin ardından güvenlik zafiyetlerinin kapatılması ve gelecekte benzer olayların önlenmesi için iyileştirmeler yapılır. Organizasyon olay sonrası süreçte elde edilen verileri kullanarak güvenlik altyapısında gerekli iyileştirmeleri gerçekleştirir. Ayrıca tehdit izleme ve analiz süreçlerinde kullanılan araçlar ve protokoller güncellenir. Güvenlik politikaları ve prosedürler, gelişen küresel tehdit ortamına göre düzenli olarak gözden geçirilir.

Sık Sorulan Sorular

Olay Müdahale Hizmeti neden önemlidir?

Olay Müdahale Hizmeti, bir organizasyonun siber tehditlere karşı hızlı ve etkili bir şekilde yanıt vermesini sağlayarak sızıntıları, veri kaybını ve operasyonel kesintileri en aza indirir. Güvenlik ihlalleri anında tespit edilip kontrol altına alındığında, saldırının olumsuz etkileri giderilebilir. Günümüzde artan siber tehditler karşısında, olay müdahale süreci bir organizasyonun siber güvenliği açısından kritik bir bileşen haline gelmiştir. Hızlı ve etkili bir olay müdahale süreci, güvenlik zafiyetlerinin giderilmesini ve saldırıların tekrarını önleyici önlemler alınmasını sağlar.

Siber olaylara nasıl müdahale edilir?

Siber olaylara müdahale, olayın tespitiyle başlar ve ardından hızlı bir analiz süreci devam eder. İlk adımda güvenlik ihlalinin kaynağı ve saldırının kapsamı belirlenerek, tehdit etkisiz hale getirilmeye çalışılır. Tehdit izole edilip analiz edilirken, saldırının olası yayılma riskleri değerlendirilir ve kontrol altına alınır. Güvenlik ekipleri, saldırının yarattığı zararları minimize etmek için gereken iyileştirme adımlarını atar. Olayın ardından detaylı bir inceleme ve raporlama süreci başlatılarak, olayın sistemlere ve uygulamalara etkisi analiz edilir.

Bir siber saldırı sırasında izlenecek ilk adımlar nelerdir?

Bir siber saldırı sırasında ilk olarak saldırının tespit edilmesi ve hızlı bir şekilde izole edilmesi gereklidir. Saldırının kaynağı ve kapsamı belirlenmeli, etkilenen sistemler hızlı bir şekilde izole edilerek olayın yayılması önlenmelidir. Olayın başlangıcından itibaren detaylı log kayıtları tutulmalı ve saldırıya dair tüm bilgiler kayıt altına alınmalıdır. Saldırının organizasyona verdiği zararın boyutu tam olarak anlaşıldıktan sonra, güvenlik iyileştirme süreçleri başlatılır. İlgili birimler ve yöneticiler bilgilendirilir ve olay raporlanır.

Olay müdahale süreci hangi aşamalardan oluşur?

Olay müdahale süreci, tehdit tespiti, ilk müdahale, analiz, izolasyon, toparlanma ve iyileştirme aşamalarından oluşur. İlk aşamada, sistemlerdeki anormal aktiviteler izlenir ve olası tehditler hızlı bir şekilde tespit edilir. İkinci adımda, tehdit izole edilerek diğer sistemlerden ayrılır ve yayılma riski önlenir. Sonrasında, olayın kaynağı ve saldırının nasıl gerçekleştiği derinlemesine analiz edilir. Analiz aşamasının ardından sistemler iyileştirilir ve güvenlik zafiyetleri giderilir.

Güvenlik ihlali durumunda kimler bilgilendirilir?

Güvenlik ihlali durumunda organizasyonun üst yönetimi, ilgili güvenlik ekipleri ve gerekli yasal düzenleyici kurumlar bilgilendirilir. İlk olarak güvenlik olayının etkilerini değerlendiren güvenlik ekipleri, üst yönetime detaylı bilgi verir. Organizasyonun içindeki ilgili birimlerle koordinasyon sağlanır ve olay hakkında sürekli bir bilgilendirme

akışı oluşturulur. Bu süreçte düzenleyici kurumlara gerekli raporlamalar yapılır ve yasal uyumluluk sağlanır.

Olay Müdahale Hizmeti nasıl test edilmeli ve güncellenmeli?

Olay Müdahale Hizmeti düzenli tatbikatlar ve simülasyonlarla test edilmeli böylece ekiplerin kriz anında nasıl tepki verecekleri ölçülür. Testler gerçek vaka senaryoları üzerinden yapılmalı ve güvenlik ekiplerinin koordinasyonu sağlanmalıdır. Her test sonrasında sürecin eksik yanları gözden geçirilmeli ve iyileştirme gerektiren alanlar belirlenmelidir. Hizmetin güncellenmesi için yeni çıkan tehditler ve saldırı teknikleri incelenerek gerekli önlemler alınır. Ayrıca, yeni güvenlik protokolleri ve teknolojiler hizmete entegre edilmelidir. Tatbikatlarda ortaya çıkan eksiklikler ve zafiyetler iyileştirilir ve müdahale prosedürleri güncellenmelidir.

Olay müdahalesinde kullanılan teknolojiler nelerdir?

Olay müdahalesinde kullanılan teknolojiler arasında SIEM (Güvenlik Bilgi ve Olay Yönetimi) sistemleri, EDR (Uç Nokta Algılama ve Yanıt), SOAR (Güvenlik Orkestrasyon, Otomasyon ve Yanıt) ve tehdit istihbaratı araçları bulunur. SIEM olayları gerçek zamanlı analiz eder ve güvenlik ihlallerini hızlıca tespit etmeye yardımcı olur. EDR çözümleri, uç noktalarda anormal aktiviteleri izler ve tehditlere karşı otomatik yanıtlar verir. SOAR platformları, olay müdahale süreçlerini otomatikleştirerek olaylara daha hızlı yanıt verilmesini sağlar.

Olay müdahalesi sırasında hangi raporlama süreçleri uygulanır?

Olay müdahalesi sırasında detaylı bir raporlama süreci uygulanarak saldırının etkisi ve zararları analiz edilir. Raporlama sürecinde saldırının kaynağı, türü, süresi ve yayılma şekli detaylandırılır. Saldırının hangi sistemlere zarar verdiği ve hangi verilerin etkilendiği belirlenir. Elde edilen tüm bilgi, belge ve bulgular ışığında, güvenlik zafiyetleri analiz edilir ve önleyici tedbirler alınır. Raporlama saldırı sonrası iyileştirme süreçlerini belirlemek ve gelecekteki tehditlere karşı önlem almak için kritik öneme sahiptir. Ayrıca hazırlanan raporlar düzenleyici kurumlar ve üst yönetim için bilgilendirici bir doküman olarak kullanılır.

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.

Privia
SECURITY