Privia SECURITY

Olay Müdahale Hizmeti

Profesyonel Forensic Hizmetleri

"Siber Krizlerde Hızlı Müdahale!"

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

+90 (216) 514 72 14

www.priviasecurity.com

"Organizasyonların siber tehditlere karşı zamanında müdahale etmesi, siber tehdidi yok etmedeki en önemli adımdır. Hızlı müdahaleyle tehditlerin etkisi hızla azaltılır, sızıntılar ve veri ihlalleri gibi saldırıların önüne geçilir."

Olay Müdahale Hizmeti, bir kuruluşun karşılaşabileceği siber güvenlik ihlallerine hızlı ve etkili yanıt vermek için hazırlanmıştır. Saldırıların yayılmasını engellemek ve sistemlerin normale dönmesini sağlamak için çeşitli teknikler kullanılır. Her türden siber olayda uzman ekiplerimiz, olaya uygun müdahale ve aksiyon planlarını devreye alır.

Olay Müdahale Hizmeti, fidye yazılım saldırıları, veri sızıntıları, DDoS saldırıları ve zararlı yazılım tespiti gibi kritik olaylar için çözümler sunar. Anlık müdahale yetenekleriyle, saldırıların etkisini en aza indirir ve iş operasyonlarının kesintisiz devam etmesini sağlar. Organizasyonun varlıklarının korunmasını sağlamak amacıyla iz kayıtları, sistem logları ve kullanıcı aktiviteleri analiz edilir. Analizler sonucunda siber saldırıların kaynağı tespit edilerek ilgili birimler bilgilendirilir. Olay müdahale sürecinde, kurum içi ve dışı paydaşlarla koordinasyon sağlanır. Yasal düzenlemelere uygun hareket edilirken, yasal regülasyonlara uygun gerekli bilgilendirmeler yapılır. Ayrıca, ulusal ve uluslararası regülasyonlara uyum sağlanması için raporlama süreçleri yönetilir.

Hizmet kapsamında sağlanan eğitim ve farkındalık programları ile organizasyonların tehditlere karşı direnci artırılır. Olay müdahale ekipleri, gelişen tehditlere uyum sağlayacak şekilde sürekli eğitilir ve simülasyonların desteğiyle tatbikatlar gerçekleştirilir. Gelecekte karşılaşılacak olası tehditlere karşı teknik ekipler güçlendirilir.

Hizmete Ait Bileşenler

Olay İzleme/İnceleme

Sistemlere yönelik anomali tespitini ve erken uyarıların iletilmesini sağlar. Log kayıtlarının sürekli izlenmesi, tehditlerin daha başlangıç aşamasında fark edilmesini mümkün kılar. Sistem üzerinde gerçekleşen şüpheli aktiviteler, olay müdahale ekibine bildirilir. Güçlü izleme araçları, saldırganların iz bırakmadan hareket etmesini zorlaştırır.

Siber Olay Müdahale Ekibi

Siber Müdahale Ekibimiz, siber tehditlere karşı hızlı aksiyon almak üzere 7/24 hazır bulunur. Her bir ekip üyesi belirli olay türleri konusunda uzmanlaşmıştır. Gerçekleşen olaylarda ekipler koordineli şekilde çalışarak krizi en kısa sürede kontrol altına alır. Olay sonrası iyileştirme sürecini de yöneterek sistemlerin eski haline dönmesini kolaylaştırır.

Forensic (Adli Bilişim) Analizleri

Olay sonrasında dijital delillerin toplanması ve analiz edilmesini sürecidir. Verilerin bütünlüğü ve hukuki geçerliliği korunarak saldırganın izleri tespit edilir. Adli bilişim uzmanları, saldırının nasıl gerçekleştiğini belirlemek için detaylı incelemeler yapar. Toplanan deliller, yasal süreçlerde kullanılmak üzere raporlanır.

Kriz Yönetimi ve İletişim Planı

Olaylar sırasında paydaşlarla etkin iletişim sağlamak için kriz yönetim planları uygulanır. İç ve dış iletişim süreçleri kontrol altına alınır. Yönetim ve/veya hukuk ekibi, gerekli durumlarda kamuoyu bilgilendirmesi yapar. Kurumun itibarını koruyacak stratejik adımlar atılır.

Olay Sonrası Raporlama

Olay müdahale süreci sonunda, gerçekleşen siber saldırılar detaylı şekilde raporlanır. Raporda saldırının türü, etkileri ve alınan aksiyonlar yer alır. Oluşturulan raporlar hem teknik hem de yönetim seviyesinde değerlendirilmeye sunulur. İyileştirme önerileri ile gelecekteki benzer olası tehditlere karşı önlem alınır.

Siber Güvenlik Tatbikatları

Siber güvenlik tatbikatları, organizasyonların siber saldırı senaryolarına karşı hazırlıklı olmasını sağlamak amacıyla düzenlenen kapsamlı tatbikatlardır. Tatbikatlar, gerçek dünya tehditlerine benzer saldırı senaryolarını içerir ve organizasyon ekiplerinin kriz anında nasıl tepki vereceğini test eder. Farklı seviyelerde düzenlenen tatbikatlar, yöneticilerden teknik ekiplere kadar tüm çalışanların dahil olduğu bir eğitim sürecini kapsar. Tatbikatlar hem teknik zafiyetlerin hem de süreçlerin eksikliklerinin tespit edilmesine olanak tanır. Ayrıca tatbikatlar düzenli tekrarlanarak, siber güvenlik ekibinin sürekli gelişimi ve güncel küresel tehditlere karşı hazırlıklı olması sağlanır.

Sık Sorulan Sorular

Olay müdahale planı (IRP) nedir?

Olay müdahale planı, bir organizasyonun siber saldırı veya veri ihlali gibi güvenlik olaylarına nasıl yanıt vereceğini özetleyen prosedürleri içerir. Olay müdahale planı, tehditlerin hızlıca tanımlanmasını, etkisinin kontrol altına alınmasını ve normal operasyonların yeniden devam etmesini sağlar. Incident Response Plan (IRP), tehditlere karşı organizasyonun hazırlıklı olmasını amaçlar. Plan kapsamında görev dağılımları, iletişim protokolleri ve teknik iyileştirme adımları tanımlanır.

Olay müdahale süreci neden önemlidir?

Siber olaylara karşı zamanında ve koordineli müdahale, saldırıların vereceği zararı en aza indirir. Etkili bir müdahale planı olmadan, veri kayıpları ve operasyonel kesintiler yaşanabilir. IRP sayesinde işletmeler, hassas bilgileri koruyarak yasal uyumluluk sağlar.

Bir olay müdahale planının geliştirilmesinde kimler yer almalıdır?

Planın hazırlanmasında siber güvenlik, SOME, veri sorumlusu, BT temsilcileri, hukuk, insan kaynakları ve halkla ilişkiler gibi farklı birimlerden temsilciler yer almalıdır. Üst yönetimin desteği de olay müdahale sürecine stratejik bir katkı sağlar ve süreçlerin sorunsuz yürütülmesini yardımcı olur.

Olay müdahale sürecinin adımları nelerdir?

Başlıca adımlar hazırlık, teşhis, sınırlama, tehdidin ortadan kaldırılması, kurtarma ve olay sonrası değerlendirme olarak tanımlanır. Hazırlık aşamasında müdahale planları geliştirilir. Teşhis, saldırının kaynağının belirlenmesini sağlar. Sınırlama ise tehdidin yayılmasını önlemeye odaklanır. Kurtarma adımında sistemler eski haline getirilir ve olay sonrası iyileştirme çalışmaları yürütülür.

Siber olaylara müdahalede SOME ekibinin rolü nedir?

Siber Olaylara Müdahale Ekibi (SOME), kriz anlarında tehditlerin analizini yapar ve müdahale stratejilerini uygular. SOME ekipleri, hem önceden tanımlanmış olaylara müdahale eder hem de gelişen küresel tehditlere karşı çözümler sunar. Adli bilişim çalışmaları ile hukuki delilleri toplayarak olası yasal süreçleri destekler.

Hangi sistem ve araçlar olay müdahalesinde kullanılır?

Saldırı tespit sistemleri (IDS/IPS), güvenlik duvarları, SIEM, DLP, EPP, EDR ve SOAR yazılımları gibi araçlar kritik öneme sahiptir. Olayların izlenmesi ve raporlanması için log yönetim sistemleri de kullanılır. Bu araçlar, tehditlerin erken görünür hale gelmesini ve etkili bir müdahale yapılmasını sağlar.

Kurumlar için siber tatbikatların önemi nedir?

Tatbikatlar, gerçek saldırı senaryolarını simüle ederek ekiplerin hazırlıklı olmasını sağlar. Tatbikatlar ile güvenlik sistemlerinin etkinliği test edilir ve eksik yönler ortaya çıkarılır. Düzenli tatbikatlar, ekiplerin gelişimini destekler ve olay müdahale süreçlerini iyileştirir.

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