Privia SECURITY

Adli Analiz Hizmeti

Profesyonel Forensic Hizmetleri

"Sayısal Delilleri Güvence Altına Alın"

Bu dokümanda yer alan bilgiler Privia Security Bilişim ve Danışmanlık Hizmetleri A.Ş. tarafından gerçekleştirilen Forensic Hizmetlere ait bilgiler olup **Genel** mahiyetindedir. Bu dokümanda yer alan tüm bilgiler, kamuya açıktır.

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

+90 (216) 514 72 14

www.priviasecurity.com

"Sayısal delillerin toplanması ve korunması adaletin sağlanması için önemli bir mihenk taşıdır. Adli analiz hizmeti ile tehditlere karşı toplanan deliller, hukuki süreçler için dayanak oluşturur."

Adli Analiz Hizmeti, dijital saldırıların izlerinin sürülmesi, elde edilen verilerin toplanarak adli süreçler için saklanması ve analiz inceleme amacıyla hazırlanmıştır. Siber dünyada yaşanan güvenlik ihlalleri sonucunda, sayısal delillerin korunması hukuki açıdan büyük önem taşır. Adli Analiz Hizmeti, özellikle veri ihlalleri, sızıntı, siber saldırılar ve kötü niyetli faaliyetlerin tespitinde kullanılacak sayısal delillerin güvence altına alınmasını sağlar.

Adli analiz süreçleri sayesinde olayın kaynağı ve saldırının detayları hakkında bilgiler, hukuki uygunluğa göre toplanır. Gerçekleştirilen analizler sonucunda, saldırının nasıl gerçekleştirildiği, hangi sistemlerin etkilendiği ve hangi yöntemlerin kullanıldığı belirlenir. Analiz süreci, saldırganın tespit edilmesi ve adli bir sonuca ulaşılabilmesi açısından kritik önem taşır. Adli analiz sürecinde kullanılan ileri teknoloji ve yöntemler, analizlerin güvenilir ve hukuki geçerliliğe sahip olmasını sağlar. Özellikle olay müdahalesi, sayısal delil toplama ve saklama süreçleri, güvenlik standartlarına ve yasalara göre gerçekleştirilir. Verilerin hukuki geçerliliğini sağlamak için delil saklama zinciri (chain of custody) gibi prosedürler uygulanır.

Adli analiz süreçleri, veri kurtarma, olay müdahalesi, iz tespiti ve dijital forensics laboratuvar çalışmaları gibi geniş bir alanı kapsar. Adli bilişim uzmanlarımız, siber olayları detaylıca inceleyerek olayla ilgili dijital delilleri raporlar ve yargıya taşınabilecek geçerli deliller sunar. Adli Analiz Hizmetiyle yasal süreçlerin ihtiyaç duyduğu, güvenilir bilgi akışı sağlanır. Adli Analiz Hizmeti, siber dünyada yaşanan olayların aydınlatılmasını sağlar.

Hizmete Ait Bileşenler

Sayısal Delil Toplama

Sayısal Delil toplama sürecinde, saldırı sonrasında dijital ortamda bırakılan tüm izler toplanır ve analiz için saklanır. Delillerin hukuki geçerliliğini korumak amacıyla, her adım dikkatlice belgelenir ve delil saklama protokollerine uyulur. Veriler, yasal süreçlerde geçerliliğini sürdürebilmesi için özel yöntemlerle korunur. Toplanan deliller üzerinde manipülasyon yapılmaz, böylece verilerin bütünlüğü korunur.

Vaka İnceleme

Vaka inceleme sürecinde, saldırının gerçekleştiği sistemler, uygulamalar, servisler ve cihazlar detaylı şekilde adli açıdan incelenir. Siber olayın kaynağını ve yayılma biçimini belirlemek için kapsamlı analizler gerçekleştirilir. Gerçekleştirilen çalışma olayın nasıl gerçekleştiğini ve hangi sistemlerin etkilendiğini tespit etmeyi amaçlar. Vaka incelemesi ile saldırganların izleri detaylandırılarak saldırının arkasındaki teknik, taktik ve yöntemler ortaya çıkarılır.

Operating System (OS) Forensics

OS Forensics, işletim sistemleri üzerinde gerçekleştirilen analizlerle, saldırganın hareketlerini ve izlerini takip etmeyi amaçlar. OS seviyesinde gerçekleştirilen adli analizler, sistem logları, kullanıcı erişimleri ve dosya işlemleri gibi bilgileri inceleyerek, saldırının detaylarını ortaya çıkarmayı hedefler. İşletim sistemindeki deliller toplanır, analiz edilir ve hukuki geçerliliği olan deliller ortaya çıkarılır. Özellikle sistemdeki iz kayıt dosyalarının bütünlüğü korunarak, sayısal delil saklama protokollerine uygun şekilde işlem yapılır.

File System Forensics

File System Forensics, dosya sistemlerinin detaylı bir şekilde incelenmesini kapsar. Saldırganın dosya sisteminde bıraktığı izler ve yaptığı değişiklikler analiz edilerek, dosya manipülasyonları, silinmiş dosyalar, zararlı dosyalar ve erişim izleri incelenir. Verilerin tam olarak ne zaman ve kim tarafından erişildiği ya da değiştirildiği gibi deliller elde edilir. File System Forensics, özellikle veri kurtarma işlemlerinde kritik bir öneme sahiptir ve dava süreçleri için hukuki deliller sağlar.

Mobile Forensics

Mobile Forensics, mobil cihazlar üzerinde gerçekleştirilen adli analizleri içerir ve cep telefonu, tablet gibi cihazlardan elde edilen sayısal delilleri inceler. Gerçekleştirilen analizlerde, cihaz içerisindeki mesajlar, çağrı kayıtları, uygulama verileri ve konum bilgileri gibi kritik veriler toplanır. Mobil cihazlarda yapılan analizler, suçla bağlantılı kişileri, olayın zamanını ve saldırganın hareketlerini belirlemede önemli bir rol oynar.

Network Forensics

Network Forensics, ağ üzerindeki veri trafiğini analiz ederek saldırının kaynakları ve yöntemleri hakkında bilgi edinmeyi sağlar. Ağ trafiğinden elde edilen veriler sayesinde, saldırganların hangi protokolleri ve bağlantı yollarını kullandığı belirlenir. Analiz sürecinde IDS/IPS logları, firewall kayıtları ve ağ geçidi bilgileri detaylı olarak incelenir. Ağ adli analizi, saldırının hangi aşamalarda ve nasıl gerçekleştiğini belirleyerek, gelecekte benzer saldırılara karşı önlemler alınmasını sağlar.

Veri Kurtarma ve Analiz

Saldırı sırasında zarar gören veya silinmiş verilere erişim sağlamak için veri kurtarma çalışmaları gerçekleştirilir. Özellikle dosya sistemleri ve yedekler üzerinde yapılan analizler, veri bütünlüğünü koruyarak kaybolan verilerin geri getirilmesine olanak tanır. Süreç içinde kullanılan özel tekniklerle, veri kaybının etkisi azaltılır ve mümkün olduğunca geri getirilir. Veri kurtarma, adli analiz sürecinde önemli bir aşamadır ve elde edilen verilerin hukuki geçerliliğini sağlamak için özel yöntemlerle korunur.

Log ve İz İnceleme

Siber olaylarda, sistem, uygulama ve servis logları/iz kayıtları saldırının kaynağını ve detaylarını anlamak için analiz edilir. Log dosyaları, hangi kullanıcıların hangi zaman dilimlerinde sistemlere eriştiğini ve neler yaptığını anlamak için kullanılır. İz kaydı inceleme çalışmaları, saldırının hangi tekniklerle gerçekleştiğini ve saldırganın nasıl bir yol izlediğini ortaya çıkarır. Gerçekleştirilen analizler, saldırganın kimliğini belirlemek veya kullandığı yöntemleri tanımlamak için oldukça önemlidir.

Adli Raporlama

Analiz sürecinin sonunda, elde edilen tüm bulgular detaylı bir rapor haline getirilir. Oluşturulan rapor, saldırının nasıl gerçekleştiğini, hangi sistemlerin etkilendiğini ve hangi adımların atıldığını raporlar. Ayrıca rapor, teknik ekipler ve hukuk birimleri tarafından incelenerek yasal süreçlerde kullanılmak üzere çoğaltılabilir. Hazırlanan raporlar, güvenilir ve doğrulanabilir nitelikte olup dava süreçleri için gerekli kanıtları içerir.

Sayısal Delil Saklama

Toplanan delillerin korunması ve hukuki süreçlerde kullanılmak üzere güvenli bir şekilde saklanması temin edilir. Delillerin güvenliği hem fiziki hem de dijital ortamda sağlanarak yetkisiz erişimlerin önüne geçilir. Güvenli saklama süreçleri, delillerin uzun süre geçerliliğini korumasını temin eder. Delillerin saklandığı ortamlar, sıkı güvenlik protokolleri ve izleme sistemleri ile korunur.

Sık Sorulan Sorular

Adli analiz nedir?

Adli analiz, siber güvenlik ihlallerini aydınlatmak ve sayısal delilleri hukuki süreçlerde kanıt olarak kullanmak amacıyla yapılan detaylı incelemeleri kapsar. Analizlerle, saldırının detayları ortaya çıkarılır, deliller toplanır ve olayın nasıl gerçekleştiği anlaşılır hale getirilir. Adli analiz, dosya sistemi, ağ trafiği, mobil cihazlar ve işletim sistemi gibi farklı dijital alanlarda incelemeler yürütür. Sayısal deliller, olayın aydınlatılmasında önemli bir rol oynar ve güvenli bir şekilde saklanarak hukuki geçerlilik sağlanır. Elde edilen bulgular yasal süreçler için raporlanır ve güvenilir kanıt niteliği taşır.

Adli analiz hangi durumlarda yapılır?

Adli analiz, veri ihlalleri, siber saldırılar, kötü amaçlı yazılımların tespiti ve veri kayıpları gibi birçok durumda gerçekleştirilir. Şirketler veya bireyler, siber saldırılara uğradığında adli analiz süreci devreye girerek saldırının detayları ve etkisi ortaya çıkarır. Adli analiz, saldırının kaynağını, kullanılan yöntemleri, teknikleri ve saldırının boyutunu anlamak için oldukça önemlidir. Özellikle hukuki süreçlerde kullanılacak delillerin toplanması ve saklanması için adli analiz kritik bir rol oynar.

Adli analiz sürecinde hangi araçlar kullanılır?

Adli analizlerde özel olarak geliştirilmiş yazılımlar ve araçlar kullanılır. Kullanılan araçlar arasında EnCase, FTK, X-Ways Forensics ve Autopsy gibi yazılımlar yer alır. Ağ trafiği analizleri için Wireshark gibi ağ izleme araçları da kullanılarak saldırı yolları ve teknikleri incelenir. Kullanılan araçlar, saldırının izlerini toplayarak kullanıcı aktivitelerini ve sistem loglarını analiz eder. Araçlar delil bütünlüğünü korumak için hash algoritmaları kullanılır.

Adli analizde delil toplama süreci nasıl işler?

Delil toplama sürecinde, olay yerinde sayısal deliller belirlenir ve uygun araçlarla toplanarak güvenli bir şekilde saklanır. Toplanan delillerin bütünlüğünü ve güvenilirliğini sağlanmak için delil saklama zinciri protokolü (“Chain of Custody”) uygulanır. Elde edilen veriler, yasal süreçlerde geçerli kanıt olarak kullanılabilmesi için özel saklama yöntemleriyle korunur. Verilerin saklanması ve korunması aşamasında, yetkisiz erişimlerin önlenmesi amacıyla güvenlik önlemleri alınır. Ayrıca, deliller üzerinde yapılan her işlem kayıt altına alınarak hukuki geçerliliği korunur.

Adli analiz raporları yasal süreçlerde nasıl kullanılır?

Adli analiz raporları, saldırının detaylarını ve sayısal delilleri açıklayan detaylı belgelerdir. Adli analiz raporları, vakanın nasıl gerçekleştiğini, hangi sistemlerin etkilendiğini ve saldırganın izlediği yolu açıklar. Adli mercilerde kullanılmak üzere hazırlanan raporlar, olayla ilgili tüm bulguları içerir ve güvenilir deliller sunar. Raporlar, yargı sürecine dahil olan tüm tarafların anlayabileceği bir formatta hazırlanarak sunulur. Ayrıca, teknik detaylar ve bulguların dayandığı deliller de rapora eklenir.

Adli analiz süreci ne kadar sürer?

Adli analiz sürecinin, olayın karmaşıklığı ve toplanacak sayısal delillerin miktarına bağlı olarak değişir. Basit bir veri ihlali durumunda analiz süreci birkaç gün sürebilirken, büyük çaplı saldırılarda aylarca sürebilir. Delil toplama, analiz ve raporlama aşamalarının her biri zaman alıcı süreçlerdir. Özellikle geniş ve dağıtık ağlar veya çok sayıda varlığın üzerinde yapılan analizler daha fazla süre gerektirir. Ayrıca bazı durumlarda sistemlerin iyileştirilmesi veya yeniden yapılandırılması da süreci uzatabilmektedir.

Adli analiz ile saldırının kaynağı belirlenebilir mi?

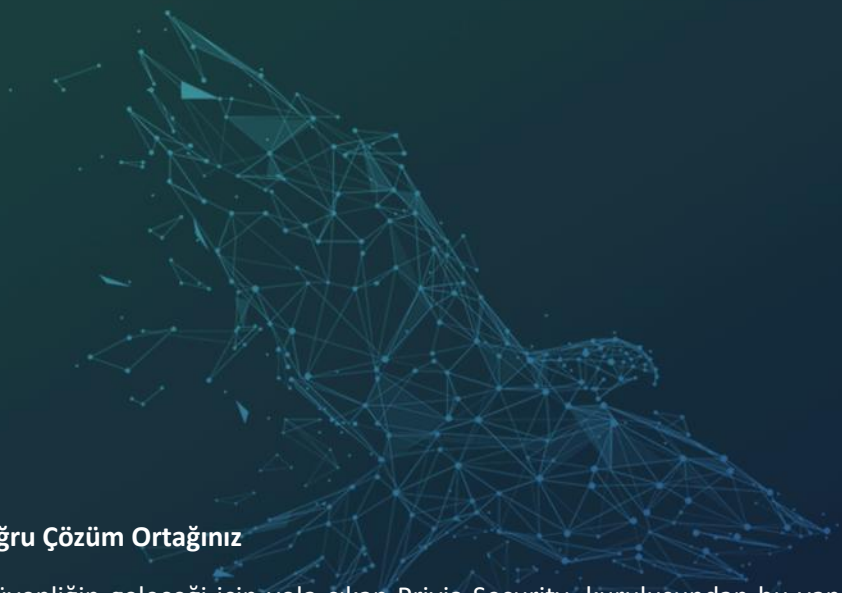
Evet, adli analiz sayesinde saldırının kaynağı büyük ölçüde belirlenebilir. Analiz sürecinde, saldırganın IP adresi, bağlantı noktaları, kullanılan zararlı yazılımlar ve sistem üzerinde yapılan işlemler tespit edilir. Elde edilen bilgiler, saldırının hangi cihazlardan başlatıldığını ve nasıl yürütüldüğünü gösterir. Özellikle ağ ve sistem iz kayıtları incelenerek saldırganın izlediği yol detaylandırılır. Kaynağın belirlenmesi, yasal süreçlerde saldırganın tespiti ve suçun aydınlatılması açısından büyük önem taşır.

Delil saklama zinciri nedir ve neden önemlidir?

Delil saklama zinciri, toplanan sayısal delillerin her adımda kimin tarafından alındığını ve nasıl işlendiğini belgeleyen bir süreçtir. Delil saklama zinciri, delillerin yasal geçerliliğini sağlamak için düzenli olarak kayıt altında tutulur. Delillerin toplanması, saklanması ve analiz edilmesi sırasında yapılan tüm işlemler kayıt altına alınarak güvenilirlik sağlanır. Zincir sayesinde, deliller üzerinde yapılan her işlem izlenebilir ve delillerin bütünlüğü korunur.

Adli analizde güvenlik zafiyetleri nasıl tespit edilir?

Adli analizde güvenlik zafiyetleri, dijital izler ve sistem logları incelenerek belirlenir. Saldırının gerçekleştiği sistemlerde yapılan detaylı analizler, saldırganların kullandığı zafiyetleri ortaya çıkarır. Özellikle ağ trafiği ve dosya sistemindeki değişiklikler incelenerek güvenlik açıklarının nerede olduğu belirlenir. Elde edilen bilgiler, olay sonrası sistem iyileştirmelerinde ve güvenlik açıklarının kapatılmasında 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