2023

ADLI BILISIM

BERKAY OZENLER

Adli Bilisim

Adli Bilisim dijital araştırılması,korunması, analizi ve sunulması ile ilgilenen adli bilisim alanında uzmanlaşmış bir alandır.

Hedef

İlk olarak hedef internet ortamından yada kişilerin cihazlarından toplanılan delillerin gerçekliğinin, bütünlüğünün oluşturulmasıdır.
Bu delillerin mahkemede kabul edilir olmasını sağlamak sonrasında siber suçlar, fikri mülkiyet hırsızlıkları, dijital hırsızlıklar ve dolandırıcılık gibi hırsızlıklıkların çözülmesine yardımcı olmaktır.
Gelişen teknolojide bu suçların artması ile adli Bilisimin önemi gün geçtikçe artmaktadır.
Siber güvelik perspektifinde bakılacak olursa adli bilisimin önemi çoğunlukla çalışanların izlenmesi ile kuruluşların yüksek seviye duruşunu devam ettirmeleridir.Bu sayede olay müdahalesinede yardımcı olur.

Adli Bilisim Türleri

Bilgisayar Adli Bilisimi	Soruşturmalara yardımcı olmak için masaüstü bilgisayarlardan, dizüstü bilgisayarlardan ve diğer bilgisayar sistemlerinden ve depolama ortamlarından alınan kanıtları belirlemek, toplamak ve saklamak.
Ag Adli Bilisimi	Ag etkinliklerinin toplanması ile ziyaret edilen web siteleri, olaylarla bağlantılı iplerin alınması, izinsiz giriş gibi tespitlerin yapılması yoluyla bilgi toplamaktır.
Bellek Adli Bilisimi	Çalışan bir sistemin Ram aracılığıyla, kanıt kurtarma işlemine verilen addır.RAM'lere öncelik verilmesi hem delil bütünlüğünün korunması anlamında hem de olası veri kaybının önüne geçilmesi anlamında önem arz etmektedir.
Mobil Adli Bilisimi	Telefon ve tablet gibi mobil cihazların servis sağlayıcı günlüklerinin incelenmesi, silinen dosyaların kurtarılmaya çalışılması, yüklenen uygulamalarının ve kalıntılarının araştırılması gibi süreçleri kapsamaktadır.

Adli Bilisimin Yararları

İyi bir Adli Bilisim kapasitesine sahip olmak, bir kuruluş için çeşitli avantajlar sağlayabilir. Uzman personel (veya eğitim) ve ekipman gerektirse de, bu maliyetler nihayetinde siber saldırıların etkisini ve olasılığını azaltarak büyük fayda sağlayabilir. Aşağıda, yararlı olmasının bazı nedenleri verilmiştir.

Olay Mudahalesini Desteklemesi

Bir olayla uğraşırken, analiz, istihbarat paylaşımı ve potansiyel kovuşturma için kullanılabilmesi için kanıtları doğru bir şekilde toplamak ve saklamak önemlidir. Dijital Adli Bilisim analistleri, derin teknik bilgilerini, analiz tekniklerini ve izleme yeteneklerini kullanarak kötü amaçlı yazılım bulaşmasından içeriden gelen tehdide kadar kötü amaçlı etkinlikleri analiz etme söz konusu olduğunda inanılmaz faydalar sağlayabilir.

Yasal Takibat

Elde edinilen bu delillerin her zaman güvenli, hesaplanabilir ve değiştirilmemiş tutulmaması halinde, mahkemede geçerli olmayacak ve bir değer taşımayacaklardır. Adli Bilisim uzmanları, delilleri uygun şekilde toplama ve ele alma konusunda bilgi sahibilerdir.Bu delilleri güvenli bir şekilde muhafaza edeceklerdir.Delillerin bu denli güvenli tutulması mahkemede geçerli olmasını sağlayacak ve değerlerinin kaybolmamasına yardımcı olacaktır.

Calısanların Izlenmesı

Bazı durumlarda, çalışanların şüpheli veya kötü niyetli davranışları nedeniyle yakından izlenmesi gerekebilir. Bu durum, iş sistemlerinde uygun olmayan internet gezintisi yapma, kabul edilebilir kullanım politikasını ihlal etme, zararlı veya uygunsuz dosyalar indirme veya güvenlik ekibinin müdahale gerektiren diğer senaryoları içerebilir. Adli Bilisim Uzmanları muhtemelen içeriden gelen tehditleri izlemek ve delilleri gizlice toplamak için eğitimli olacaklar ve bu deliller, İnsan Kaynakları departmanının bir çalışanı işten çıkarmak için haklı göstermesi veya kullanıcının faaliyetlerinin yasaları ihlal etmesi durumunda yasal makamlara teslim edilmesi amacıyla kullanılabilir.

Adlı Bılısım Ilıskılı Roller

T1 SOC ANALISTI	T1 Analistleri genellikle başlangıç araştırmalarını yürütür, çoğunlukla birinci seviye olay yanıtı sağlar ve bir soruşturma dosyasına eklenecek delilleri toplar. Bu deliller daha sonra, IP adresini, alan adını engelleme gibi savunma tedbirlerinin haklı gösterilmesinde kullanılır.
T2-3 SOC ANALISTI	T2/T3 Analistleri genellikle daha teknik uzmanlık gerektiren veya ek araçlara ve sensörlere erişim izni olan daha kritik soruşturmaları ele alırlar. Kritik ve yüksek öncelikli soruşturmaların doğası gereği, ilgili delillerin daha sıkı koşullar altında toplanması ve ele alınması gerekecektir.
KOTU AMACLI YAZILIM ANALISTI	Güvenlik operasyonları alanında, Dijital Adli bilisim terimi, kötü amaçlı yazılım analizi sürecine de atıfta bulunmak için kullanılabilir. Kötü amaçlı yazılımın bir örneğini alarak ve farklı teknikleri kullanarak amacını keşfetmek ve gelecekte IOCs (Güvenlik İhlal Göstergesi) toplayarak onu nasıl tespit edeceğimizi öğrenmek için kullanılır.
ADLI BILISIM Uzmanı	Dijital Adli Bilisim Uzmanları, yüksek profilli soruşturmalar, yükseltilmiş vakalar, çalışan izleme, Güvenlik Olay Yanıt Ekibi (SIRT) ile birlikte çalışma ve güvenilir ve yüksek teknik bilgiye sahip kişiler gerektiren diğer görevler üzerinde çalışacaktır.
IC TEHDIT ANALISTI	İç tehditleri tespit ve izlemeye odaklanan güvenlik uzmanları, geniş dijital adli bilisim becerilerini kullanarak hiçbir detayı gözden kaçırmayacak ve bir kişiye karşı olan tüm delillerin uygun şekilde toplandığından emin olacaklardır.
TEHDIT AVCILARI ★	Tehdit Avcıları, uzman teknik savunucular olarak hem saldırgan hem de savunma uygulamalarını derinlemesine anlayan kişilerdir. Bu bireyler, etkili bir şekilde avlanabilmek için bilgisayarların ve ağların işleyişini gerçekten anlamalı ve aynı zamanda sızıntının kanıtı olarak bulunabilecek önemli izleri anlayabilmelidirler.
OLAY MUDAHALE UZMANI	Olay Mudahale Uzmanları genellikle ileri seviye mavi takım yeteneklerine sahip üst düzey güvenlik analistleridir, bunlardan biri de adli Bilisimdir. Bu, sistemlerin nasıl tehlikeye düştüğünü ve cihaz davranışını anlamak için daha derin ve detaylı soruşturmalar yapmalarına olanak sağlar.

TESEKKURLER