OSINT
AÇIK KAYNAK İSTİHBARATI

Rapor

Berkay Ozenler
Cyber Security Specialist

AUGUST 2023

OSINT

Tanım

Açık Kaynak İstihbaratının kısaltması olan OSINT, halka açık kaynaklardan elde edilen verilerdir . OSINT, kolluk kuvvetleri işlerinde, saldırı planlama gibi siber suç faaliyetlerinde veya rekabeti kontrol etmek gibi iş operasyonlarında yaygın olarak kullanılmaktadır.

Ornekler

Çalışanlarını web sayfasında tanıtan bir şirket düşünürsek bu şirket istemeden de olsa saldırganların bu kişiler hakkında bilgi toplamasına olanak tanımıştır.

Kuruluşlarının işleyişi hakkında bilgi tanımı, sistem tanımı yapan şirketler, bu bilgi ve sistem tanımlamalarını yapan şirketler aslında bir saldırganın içeriye sızdığında yapacağı erişim yükseltme gibi saldırı tekniklerini daha iyi bir şekilde uygulamasına olanak sağlar.

Sosyal medyada paylaşılan lokasyon bildiren fotoğraflar, bu şekilde paylaşılan fotoğraf yada veriler kişi hakkında anlık bilgi toplamaya ve kişinin hayatının işleyişi yani nerde, ne zaman, nasıl gibi sorulara tanımlamalar yapmaya yarar.

Bir kullanıcı yada kişi hakkında bilgi toplamak için kendisinin sosyal medya profillerini incelemek, kişi hakkında doğum tarihi, aile bilgileri, nerde yaşıyor gibi bilgileri açık olarak sunmasıyla gerçekleşen bilgi toplama çeşididir.

Siber Sucluları ortaya çıkarmak, Bu, Tehdit İstihbaratı alanına kaymaya başlasa da, siber suçluların gerçek kimliğini belirlemek ve ayrıntıları kolluk kuvvetlerine iletmek için OSINT kaynaklarını ve sosyal mühendislik becerilerini kullanmak mümkündür.

Görüldüğü üzere bu tarz bilgi toplama, sosyal mühendislik işlemleri ile kişi yada kuruluşlar hakkında saldırı yapılmadan bu saldırıya nasıl ve ne şekilde hazırlanılacağı tasarlanabilir. Siber Guvenlik ile ilgili alanlarda ise saldırganlar hakkında bilgi toplanabilir ve kişisel bilgilerine erişim sağlanıp kolluk kuvetleriyle paylaşılabilir.

OSINT NEDEN YARARLI

Siber Güvenlik Bakış Açısı

İnternette bulunan bilgileri gözden geçirerek veya diğer kontrolleri uygulayarak saldırıyı hafifletmek veya etkinliğini azaltmak için adımlar atabilirler. Bir saldırganın çalışanlar hakkında ayrıntılı profiller oluşturması çok tehlikeli olabilir. Ancak, bu çalışanın güvenlik eğitimi alması halinde, potansiyel olarak kötü amaçlı e-posta ve sosyal mühendislik saldırılarını daha iyi tespit edebilecektir.
Bir saldırgana yardımcı olabilecek çevrimiçi bilgileri kaldırarak, saldırı yüzeyini veya bir saldırganın dahili sistemlere erişim elde etmek için yararlanabileceği toplam gücü azaltır.

Kolluk Kuvetleri Bakış Açısı

Hükümet ve kolluk kuvvetleri OSINT'i suçluları, şüphelileri, teröristleri ve diğer ilgili kişileri izlemek için kullanır. Profil oluşturma, kişiliklerini ve davranışlarını anlamak için bireyler hakkında bilgi toplar. Bu, kullanıcının ilgi alanlarına ve önceki konumlarına göre belirli bir zamanda nerede olacağını tahmin etmek için kullanılabilir. OSINT, zayıf OPSEC'ye (Operasyonel Güvenlik - kişinin çevrimiçi kimliğini gerçek benliğinden ayırarak çevrimiçi saklama eylemi) sahip siber suçluların kimliklerini ifşa etmek için kullanılabilir. Ayrıca, kayıp kişilerin bulunmasına yardımcı olmak için de kullanılabilir (buna iyi bir örnek, çevrimiçi OSINT CTF'ye ev sahipliği yapan kar amacı gütmeyen bir kuruluş olan ve aslında kayıp kişi izleme ve yasa uygulama kurumu olan Trace Labs'dır.

Isletmelerin Bakıs Açısı

İşletmeler OSINT'i rekabeti izlemek, pazar etkinliğini izlemek, OSINT'in müşterilerle en iyi nasıl etkileşim kurabileceği hakkında daha fazla bilgi edinmek, veri zenginleştirme yoluyla operasyonları iyileştirmek ve ayrıca kimlik bilgileri ve çalışan güvenliğini azaltmak için kullanır. Hassas bilgileri veya saldırıyı planlayan bilgisayar korsanı. Bunun önemli bir kısmı, ne yaptıklarını görmek için rakiplerinizin sosyal medya kanallarını izlemektir. Bu, şirketinizin sosyal medya ve pazarlama stratejisini desteklemek için kullanılabilir.

OSINT NEDEN YARARLI

Saldırganların Bakış Açısı

OSINT kaynakları, şirketler ve ilgili kişiler hakkında bilgi bulmanın harika bir yoludur. Kuruluşunuzun hangi sistemleri kullandığını bilmek, uygun açıklardan yararlanma ve saldırı yöntemleri için önceden plan yapmanızı sağlar. Çalışan bilgilerinin toplanması, potansiyel olarak etkili sosyal mühendislik saldırılarının yanı sıra amaçlanan hedeften daha güvenilir olan spear phishing e-posta oltamalarına izin verir. İşletmeler, sistemleri ve çalışanlarının çevrimiçi paylaştığı bilgiler konusunda dikkatli olmalıdır. Bu bilgilerin kötü niyetli amaçlarla toplanma süreci genellikle hedefli istihbarat toplama veya pasif istihbarat toplama olarak adlandırılır (çünkü saldırgan, hedefin sistemiyle bağlantı noktası, güvenlik açığı taraması vb. aracılığıyla doğrudan etkileşime girmez).

Ilişkili Roller

OSINT'i belirli işlevler için kullanan çeşitli roller vardır. En önemlisi, tehdit istihbaratı analistleri, güvenlik araştırmacıları ve penetrasyon testçileri OSINT'i sektördeki diğer rollerden daha fazla kullanıyor.

Taktiksel Tehdit Analisti

Taktik tehdit analistleri, istihbarat operasyonlarını yürütmek ve kuruluşlarını hedef alabilecek düşmanlar hakkında bilgi toplamak için OSINT'i kullanabilir. Kötü niyetli aktörleri izleyerek, bu grupların karşı önlemlerini uygulamak için kullandıkları en son trendleri ve teknikleri takip ediyoruz.

Ayrıca OSINT kaynaklarından IOC'ler toplayabilir ve bunları dahili olarak tehdit kontrolleri yapmak için kullanabilirsiniz.

Stratejik Tehdit Analisti

Bir Stratejik Tehdit Analisti, bir tehdit değerlendirmesi yapabilir ve kuruluşunuzun İnternet'e hangi bilgileri "sızdırdığını" belirleyebilir. Buna dahili sistemler, sosyal medyada rozetlerin resimlerini gönderen çalışanlar (kötü niyetli saldırganlar bu rozetleri kopyalayabilir ve sosyal mühendislik saldırıları için kullanabilirler) ve internette yardımcı olabilecek bilgilerin bulunduğu diğer durumlar ile ilgili bilgiler olabilir.

Güvenlik Analisti

Güvenlik analistleri OSINT verilerini, IP adreslerinin itibarını (VirusTotal, IPVoid) ve e-posta adresleri ve dosya karmaları (VirusTotal, IBM X-Force Exchange) gibi IOC'leri kontrol etmek de dahil olmak üzere çeşitli nedenlerle kullanır. Diğer kullanım örnekleri, çalışanlara yönelik sosyal mühendislik saldırılarında kullanılan sahte sosyal medya hesaplarının araştırılmasını içerir.

Zafiyet Analisti

OSINT bu rolün önemli bir parçasıdır. En son yayınlanan güvenlik açıklarından haberdar olmak, güvenlik açığı araştırmacılarını sosyal medyada takip etmek ve bilgi paylaşmak yaptıkları işin çok önemli bir parçasıdır. Harika bir OSINT kaynağı, Twitter güvenlik açığı haberlerini ve açıklamalarını izlemek için TweetDeck'i kullanan Ulusal Güvenlik Açığı Veritabanıdır.

Pen Tester /Red Teamer

Penetration Testerlar, iç sistemler ve çalışan bilgileri dahil olmak üzere hedef şirketler hakkında bilgi almak için OSINT'i kullanır. Saldırıları özelleştirmek, saldırıların oluşturduğu etkiyi,sesi (hedefin farkında olmamasını sağlayacak işlemler) azaltmak, başarı şansını arttırmak için ve penetrasyon oranını yükseltmek için kullanılır.

Zeka Döngüsü

İster kolluk kuvvetlerinin bir üyesi olun ister bir kurumsal güvenlik analisti olun, her iki senaryoda muhtemelen aynı durumla karşı karşıya kalırsınız. Bir yandan çok büyük miktarda veriyi analiz etmeniz, diğer yandan sorunları çözmemiz gerekiyor.
Bu senaryonun üstesinden gelmek için, elinizin altındaki çok büyük miktardaki veriden faydalanmanız ve aradığınız çözümleri ifade eden istihbarat raporları oluşturmak için kullanmanız gerekir.
Bununla ilgili tek sorun, istihbarat raporlarının kendi kendine oluşmamasıdır. Yani sadece tüm bu verileri tanımlamamız gerekmiyor, aynı zamanda onları bilgiye dönüştürülebilecek şekilde kategorize etmeniz ve düzenlemeniz gerekiyor.
Bu tür durumlar için her zaman Zeka Döngüsü adı verilen bir bilgi oluşturma süreci vardır. Bu model, araştırmacıların topladıkları verileri ve bilgileri kuruluşlarına çözüm sağlayabilecek istihbarat ürünlerine dönüştürmek için atmaları gereken bir dizi adımı ve prosedürü tanımlar.

Gerçekleşmesi Için Gereken Adımlar

Planlama ve Oryantasyon

Bu ilk aşama, araştırmanın hangi alanları izleyeceğini belirlediği için araştırma sürecinin önemli bir bileşenidir.Burada, araştırmanızın amacını ve aradığınız bilgi türünü tanımlarsınız.

Toplama (veri ve bilgi toplama)

Bu ikinci aşamanın amacı, bu bilgileri toplamak için hangi süreçlerin kullanılacağını belirlemek ve istihbarat operasyonlarının yürütülmesinde yararlı olan verileri elde etmek için bilinen herhangi bir tekniği kullanmaktır.

Veri ve bilgilerin işlenmesi

Bu aşama, önceki süreçte gerçekleştirilen herşeyi ele alır.
Buradaki amaç sadece bilgiyi görselleştirmek değil, aynı zamanda deşifre etme, doğrulama ve değerlendirme tekniklerini uygulayarak bilgi yığınlarını filtreleyebilmek, tanımlayabilmek ve edindiğimiz faydalı verileri araştırabilmektir.

Anlamlı bilgiler oluşturmak için analitik çözümler

Analistlerin gerçekte ne olduklarını gösterebilecekleri yer burasıdır.

Burada bir önceki adımda süzdüğünüz tüm bilgileri derleyerek baştaki probleminizin çözümlerini elde etmeniz ve son zamanlarda yaşadığınız süreci net bir şekilde anlatabilmenizi sağlayan tutarlı bir istihbarat ürünü (rapor, konferans vb.) oluşturmanız gerekmektedir.

Bilgilerin müşterilere iletilmesi

Son adım. Burada süreç boyunca geliştirilen ürün, talep eden ilgili taraflara (birey veya gruplara) teslim edilmelidir. Bu, problem üzerinde çalışırken iyi ve bilinçli kararlar vermenize yardımcı olacaktır. Bu Zeka Döngüsünün tanımı diyebiliriz.

Devamı uygulamalarla donatılıp eklenecektir