ÇÖZÜM NOTU

INFOBLOX DOSSIER™

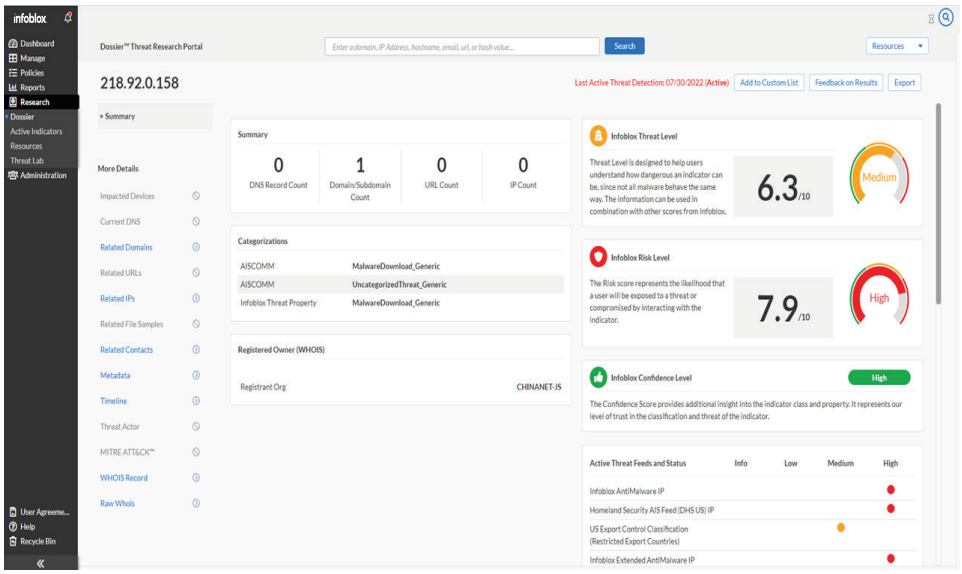
Daha hızlı yanıtlar. Daha fazla bağlam. Daha iyi kararlar.

IoC'LERDEN DAHA FAZLASI

Threat Intelligence (TI) bir zamanlar kötü amaçlı yazılım karmaları, kötü niyetli URL'ler ve diğer IoC'lerden (Güvenlik İhlali Göstergeleri) biraz daha fazlasını içeriyordu. Ancak günümüzün savunucuları, savunmaları etkili bir şekilde hazırlamak, saldırıları tespit etmek, araştırmak, avlamak veya modern, karmaşık, çok aşamalı siber saldırılara yanıt vermek için genellikle bir tehdit ve arkasındaki aktörler hakkında çok daha derin bir anlayışa ihtiyaç duyuyor. Bunu yapmak için genellikle küçük bir portal cephaneliğine, çeşitli TI kaynaklarına ve mevcut ilgi tehdidi hakkında gerekli içgörüyü bulma umuduyla bu farklı kaynaklardan gelen verileri filtrelemek ve ilişkilendirmek için çok fazla zaman harcamaları gerekir.

SECOPS'U DAHA VERIMLI HALE GETIRMEK

BloxOne® Threat Defense, analistlerin, tehdit araştırmacılarının, güvenlik personelinin ve diğer SOC ekip üyelerinin çabalarını kolaylaştırmak ve düzenlemek için güçlü bir tehdit araştırma aracı olan Dossier'i sunar. Seçtiğiniz düzinelerce açık kaynak, tescilli veya premium ticari kaynaktan threat intelligence toplanmasını ve ilişkilendirilmesini otomatikleştirir. Tüm bu bilgileri tek bir görünümde sunarak, ekibinizin araştırmaları daha hızlı tamamlamak ve daha hızlı ve etkili yanıt vermek için gereken içgörüler için mevcut verilerden yararlanmasına olanak tanır.



Şekil 1: Ortaya çıkan bir tehdidin dosya özeti ve mevcut veriler arasında kolayca yönlendirme yapabilmek için bağlantılar

GERÇEKLER VE RAKAMLAR

- Dossier, tehdit araştırma, inceleme ve müdahale çalışmalarının hızını, kalitesini ve doğruluğunu yüzde 67'ye kadar artırır.
- Dossier, daha fazla güvenle daha hızlı ve anında eyleme geçirilebilir kararlar almanızı sağlar.
- Güvenlik ve risk liderlerinin yüzde 74'ü, ortalama bir tehdit soruşturmasının dört saatten uzun sürmesinden şikayetçi.
- Uygulayıcıların yüzde 64'ü güvenlik soruşturmasının yoğun kaynak gerektirdiğini söylüyor.

*Kaynak: Forrester Research Nisan 2020, Ponemon Institute 2019, ISC2 Siber Güvenlik İşgücü Araştırması, 2019

GÜÇLÜ KULLANIM SENARYOLARI EYLEME GEÇIRILEBILIR VERILERDEN YARARLANIR

BloxOne Threat Defense'in Infoblox Dossier özelliği, BloxOne Threat Defense ile yerel entegrasyon sayesinde araştırma verilerini doğrudan DNS düzeyinde eyleme geçirilebilir hale getirir. Dossier'in doğrudan entegrasyonu, araştırmacıların tehdidi hemen bir engelleme listesine eklemelerine olanak tanır. İnfoblox Dossier'in hızını, kullanım kolaylığını ve önemli avantajlarını göstermek için dört önemli kullanım örneği şunlardır:

Kullanım Örneği #1

Belirli Bir Tehdit Göstergesi için Göreceli Tehdit ve Risk Düzeyini Anlayın

Bankanızın güvenlik operasyonları ekibi, birkaç departmandaki birçok kişi tarafından alınan spam e-postayla ilişkili şüpheli bir URL'yi tespit etti. Olası tehdit ve risk seviyelerini anlamak istiyorsunuz. URL'yi Dossier'e girer ve göstergeyle ilgili diğer önemli bağlamsal verilere hızlıca erişirsiniz. Bu URL, Dossier'in bazı threat intelligence kaynakları tarafından kötü amaçlı bir web sitesi olarak rapor edilmiş ve bankacılık Truva atları ile ilişkilendirilmiştir. Tehdit ve risk yüksek olduğundan bu tehdidi gidermek için harekete geçmelisiniz. Alan adını engelleme listenize tek bir adımda eklersiniz. BloxOne Threat Defense, her yerdeki tüm kullanıcıları ve cihazları bu kötü amaçlı alan adına yanlışlıkla erişmekten derhal korur.

Kullanım Örneği #2

CISA Uyarısından Tanımlanan Bir Tehdidin Sızma Derecesini Ortaya Çıkarın

Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA), belirli bir tehdit aktör grubunun hastanelere yönelik saldırıları hakkında bir uyarı yayınladı. Uyarıda çeşitli tehdit göstergeleri yer alıyor. Bu tehdidin hastanenizi etkileyip etkilemediğini mümkün olan en kısa sürede öğrenmeniz gerekir. Dossier içinde tehdit göstergelerini araştırmak için yön değiştiriyor ve bunun threat intelligence feed'lerinizin birçoğu tarafından zaten tanımlandığını ve engellendiğini görüyorsunuz. Dossier içinde etkilenen cihazlara gidip kuruluşunuzda bu IP göstergelerinin hiç kullanılmadığını görebilirsiniz. Kuruluşunuzun şu anda bu tehditten etkilenmediğini derhal öğrenirsiniz.

Kullanım Senaryosu #3

Riski Değerlendirmek için Alan Adı Kaydı ile Alan Adı Barındırma Arasındaki Farkı Hızla Belirleyin

Ekibiniz, ekip üyelerinizden birinin eriştiği küçük işletme web sitesiyle iletişim kuran belirgin bir kötü amaçlı yazılım fark etti. Bu web sitesi URL'si tehdit feed'lerinizin hiçbirinde tanımlanmamıştır. Konum verileriyle ilgili bağlamsal bilgilere döndüğünüzde, bu yerel küçük işletme web sitesinin bir ülkede kayıtlı ancak başka bir ülkede barındırılan bir alan adına sahip olduğunu görürsünüz. Bu konum verileri potansiyel olarak tehlikeli bir tehdidin geçerliliğini doğruluyor gibi görünüyor ve alan adını hemen izleme listenize ekliyorsunuz.

Kullanım Senaryosu #4

Kuruluşunuzdaki Bir Tehditin Geçmişteki Etkinliğinin İzini Sürün

Kısa bir süre önce işletmenizde kötü amaçlı birkaç bilgi hırsızlığı keşfettiniz. Ekibiniz, Dossier içinde daha önce ne kadar etkinlik gerçekleşmiş olabileceğini anlamak için ek araştırmalar yapar. Tehdit aktörleri, alan adı süresinin dolmasını sık sık izler ve meşru sahibi tarafından zamanında yeniden kayıt yapılmadığında web sitelerini yeniden kaydetmek için hızlıca harekete geçer. Dossier, tehditle ilişkili önemli olayları gözden geçirmek için Dossier zaman çizelgesine geçiş yapmanızı sağlar. Ayrıca alan adı kaydını gözden geçirebilir ve bir riske işaret edebilecek sahiplik değişikliklerini tespit edebilirsiniz.

Kullanım Senaryosu #5

Müdahale Etkinliklerini MITRE ATT&CK™ Çerçevesiyle Hızlıca Uyumlu Hale Getirin

Gerçek bir ihlale yanıt olarak veya bir tehdit avlama tatbikatını desteklemek amacıyla Dossier, saldırgan tekniklerini sınıflandırmak, incelemek ve niyetlerini anlamak için güçlü bir yöntem olan MITRE ATT&CK çerçevesinden mevcut rehberlik sunar. Bu rehberlik, kontrol altına alma ve diğer olay müdahale faaliyetlerini hızlandırmak ve optimize etmek açısından yardımcı olabilir. Yalnızca mevcut aramayla ilgili MITRE ATT&CK araçları görüntülenir. Bu sayede tehdit avlama ve algılamak çabalarınızı geliştirmek, analiz ve test etmek için MITRE ATT&CK'i kullanabilirsiniz.

DAHA ETKILI ARAŞTIRMALAR VE SORUŞTURMALAR

Dossier tarafından otomatik olarak toplanan ve düzenlenen verilerle çalışarak bir tehdidin farklı yönlerini araştırın, izi takip ederek tehdidi nasıl daha etkili bir şekilde korunacağınızı, tespit edeceğinizi veya yanıt vereceğinizi daha iyi anlayın. Toplanan ve adresinden isteğe bağlı erişime sunulan temel veri alanlarından bazıları şunlardır.

Etkilenen Cihazlar

Bu liste, araştırmakta olduğunuz gösterge için bir sorgu çalıştırılarak oluşturulmuştur. Veriler raporlama günlüklerinden gelmektedir. Görüntüleme, son 30 gün içinde yapılan sorgularla sınırlıdır. Bir tehdit bulursanız, uzaktaki ana bilgisayarla hangi cihazların temas ettiğini belirlemek son derece faydalıdır.

Özel Listeler

Aboneliğinizin sunduğu önceden tanımlanmış threat intelligence feed'lerine ek olarak, daha fazla koruma sağlamak için izin listeleri ve engelleme listeleri tanımlamak üzere alan adları ve IP adresleri içeren özel listeler oluşturabilirsiniz. Mevcut feed'leri tamamlamak veya mevcut bir feed için tanımlanmış Engelle, İzin Ver, Günlüğe Kaydet veya Yönlendir eylemini geçersiz kılmak üzere özel bir liste kullanabilirsiniz. Dossier, iki basit tıklama ile özel listeleri düzenlemenize olanak tanır.

Benzerlik Tespiti

Infoblox tarafından izlenen ilk 1.000 global alan adının benzerleri tespit edilmiştir. BloxOne Threat Defense Advanced ile, benzerlik etkinlikler için izlenmesini istediğiniz diğer özel alan adlarını eklemek üzere bu özelliği genişletebilirsiniz.

İlgili Kişiler

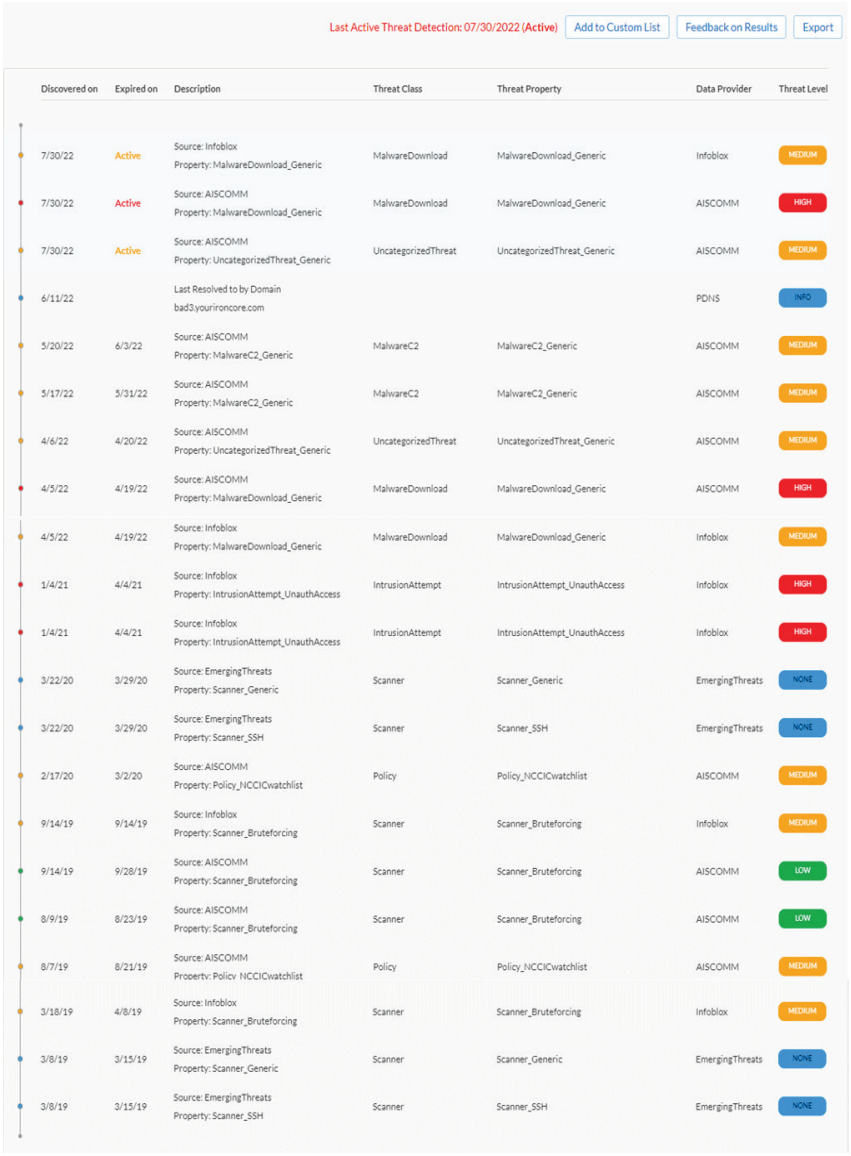
İlgili Kişiler, Alan Adı kayıt ayrıntılarına göre kayıtlı kişileri gösterir. Birçok alan adı sınırlı ayrıntılar gösterse de, e-posta adresi veya telefon numarası bazen birden fazla alan adını tek bir sahibine bağlamak için yararlıdır. Başarılı bir saldırgan genellikle yüzlerce alan adına sahiptir.

Meta veri

Raporlar, webdeki göstergeyle ilgili web içeriğini gösterir. Bunlar, filtrelenmedikleri ve bu göstergenin doğası hakkında genel bir bakış açısı sağlamak üzere listelendikleri için kötü amaçlı olabilir.

Zaman Çizelgesi

Bu özellik, tehdit etkinliğindeki önemli olayları ve alan adı kayıt geçmişini gösterir. Sahiplik değişikliklerini tespit edebilirsiniz. Kaynaklar arasında WHOIS (gerçek kayıtlar), PDNS (gerçek trafikten gözlemlenen pasif DNS) ve alan adlarını yeni oluşturulduğunda izleyen SURBL gibi çeşitli feed'ler bulunmaktadır.



Şekil 2: Kötü amaçlı etkinliklerin uzun geçmişi, tespit edilen tehdit etkinliğinin kaynağı etrafında ortaya çıkar.

Mevcut DNS Kayıtları

Yaygın DNS kayıt türlerine hızlı bir bakış, uzak bir ana bilgisayardaki hizmetler hakkında size çok şey anlatır. Mail Exchanger (MX) ve web sitesi olmaması (A), genişletilmiş DNS alanları, uzak ana bilgisayar/alan adının amacı hakkında bir hikaye anlatır.

İlgili Alan Adları

Bu alan adları, birden fazla alan adı kullanan kötü amaçlı yazılımlar gibi birçok olası ilişkilendirmeye dayalı olarak araştırılan göstergeye bağlanmıştır.

İlgili URL'ler

Bu web siteleri, kötü amaçlı yazılım veya spam gibi birçok olası ilişkilendirmeye dayanarak araştırılan göstergeyle ilişkilendirilmiştir.

İlgili IP'ler

Bunlar bu alan adıyla ilişkilendirilmiş IP adresleridir.

İlgili Dosya Örnekleri

Bu örnekler, alan adı/IP ile doğrudan ilişkili olabilecek kötü amaçlı dosyalara dayanmaktadır. En yaygın kaynak, alan adından gelen veya alan adıyla iletişim kuran dosyalar hakkında rapor veren kötü amaçlı yazılım (virüs) motorları olacaktır.

MITRE ATT&CK™

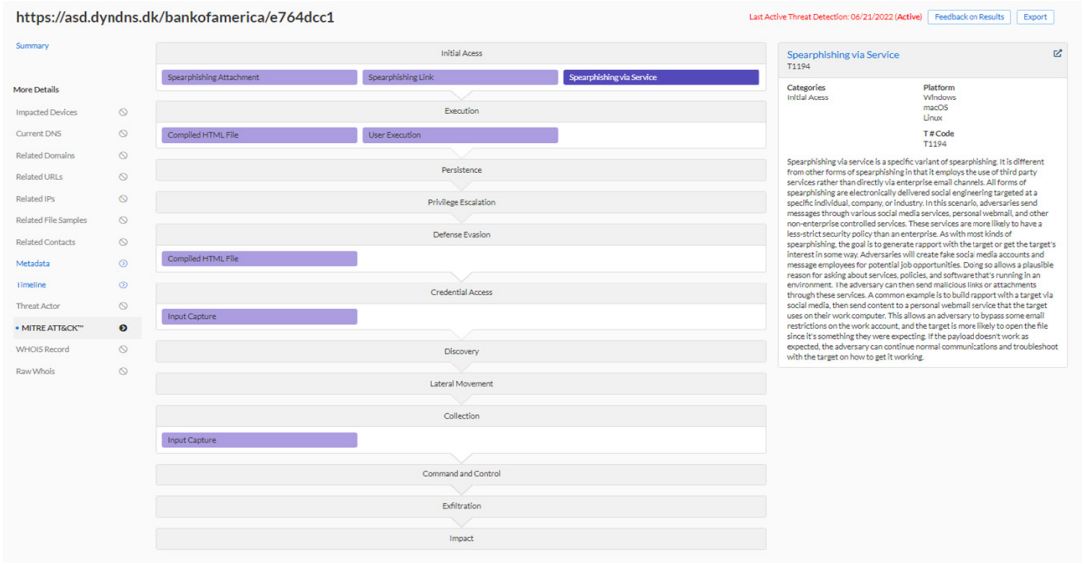
MITRE ATT&CK™, gerçek dünya gözlemlerine dayanan saldırgan taktikleri ve tekniklerinin küresel olarak erişilebilir bir bilgi tabanıdır. Yalnızca mevcut aramayla ilgili MITRE ATT&CK araçları görüntülenir. Bu sayede tehdit avlama ve algılama çabalarınızı geliştirmek, analiz etmek ve test etmek için MITRE ATT&CK'i kullanabilirsiniz.

Tehdit Aktörü

Göstergeyle ilgili bir tehdit aktörü hakkında veri mevcutsa gösterilecek ve vurgulanacaktır. Bu, onlar, araçları, yöntemleri ve saldırı için olası motivasyonları hakkında bilgi edinmenize yardımcı olur.

WHOIS kaydı

WHOIS Kaydı, birden fazla alan adı kayıtlarından ve Internet IP yetkililerinden elde edilen kamu kayıtlarına dayanmaktadır. Farklı yetkililer daha fazla veya daha az veri sağlar ve bazı durumlarda neredeyse anonim kayda izin verir. Alan adlarını veya IP'leri araştırmak için WHOIS kaydını kullanırken, "kötüye kullanım" iletişim e-postası ve alan adı sunucuları gibi verileri dikkatlice inceleyin, çünkü bu bilgiler sizi gerçek sahibe yönlendirebilir.



Şekil 3: İncelenen tehdide göre, bu rapor MITRE ATT&CK çerçevesinden rehberlik sunmaktadır.

DIZIN KAYNAĞI AÇIKLAMALARI

Dossier tehdit göstergesi araştırma aracı birden fazla kaynak kullanır. Dossier araç setini kullanarak, kullanıcılar aynı anda bir düzine kaynaktan elde edilen bağlamsal bilgilere dayanarak daha hızlı ve daha fazla güvenle doğru kararlar alabilirler. Dizin kaynak açıklamaları şunları içerir:

Infoblox Siber İstihbarat Birimi (CIU)

CIU, Infoblox müşterilerine sağlanmak üzere tehdit araştırması (avlama, soruşturma vb.), algılama teknolojileri (Yapay Zeka, Makine Öğrenimi vb.) ve düzinelerce kaynaktan threat intelligence'ın toplanması ve düzenlenmesinden sorumlu Infoblox tehdit araştırma ekibidir. Bu çalışma, Dossier'in soruşturma yeteneklerini ve BloxOne Threat Defense'in savunma yeteneklerini güçlendirir.

Mevcut DNS

Mevcut DNS arama sonuçları, DNS ad sunucularından belirli bir ana bilgisayar adı hakkında mevcut tüm bilgileri sunar.

Metadata

Bu araç, aradığınız göstergeyi bahseden veya ona bağlantı veren web'deki ilgili makalelere tek bir görünüm sunar. Analistlere, potansiyel olarak zararlı bağlantıları takip etme riski olmadan bu bilgilere erişebilmeleri için güvenli bir ortam sağlanır.

Coğrafi konum

Coğrafi konum aracı, tespit edilen koordinatları bir harita üzerinde gösterir ve şehir düzeyinde hassasiyet sağlar. Diğer bilgiler arasında ISP, şehir, bölge, enlem/boylam ve ülke bulunur.

Google Safe Browsing

Google Safe Browsing veya GSB, uygulamaların URL'leri Google'ın sürekli güncellenen şüpheli kimlik avı, kötü amaçlı yazılım ve istenmeyen yazılım sayfaları listelerine karşı kontrol etmesine olanak tanır.

Infoblox InfoRanks

InfoRanks listesi, çeşitli veri kaynaklarından alınan DNS kayıtlarına dayalı birleştirilmiş bir veri kümesinden her gün güncellenen en popüler ikinci düzey alan adlarını (SLD'ler) sunar. Her bir alan adının sıralamasını belirleme süreci, SLD'lerin zaman içindeki gerçek sıralamalarını doğru bir şekilde tahmin etmek için sayım bilgilerini istatistiksel çıkarım teknikleriyle birleştirir ve bu da onu artık kullanılmayan Alexa sıralamasının yerine güçlü bir alternatif yapar. Sütun başlığına tıklayarak sonuçları Alan Adı veya Sıralamaya göre filtreleyebilirsiniz.

Pasif DNS

Pasif DNS, ana bilgisayar adları için tarihsel DNS kaydıdır. Bir ana bilgisayar adını aradığınızda, Pasif DNS, ana bilgisayar adının çözümlendiği ve önceki 12 ay içinde Pasif DNS sensörleri tarafından tespit edilen tüm IP adreslerini döndürecektir. Bir IP adresi arandığında, Pasif DNS, o IP'ye yönlendirilmiş tüm ana bilgisayar adlarını döndürecektir. Her DNS değişikliğinin yakalanmadığını, bu nedenle eksik bilgiler olacağını unutmayın.

Ters DNS

Ters DNS aracı, alan adı kayıt defteri ve kayıt kuruluşu tablolarını arayarak bir IP adresinin ters DNS aramasını gerçekleştirir.

Ters Whois

Bu araç, güncel veya geçmiş Whois kayıtlarında listelenen kayıt sahibinin adı, adresi, telefon numarası, e-posta adresi veya fiziksel adresi gibi bilgiler sağlar.

Zararlı Yazılım Analizi

Kötü amaçlı içeriğin veri toplaması, virüsten koruma motorlarının ve web sitesi tarayıcılarının toplanmasıyla algılanır.

Whois

Whois, bir alan adının sahibini ve iletişim bilgilerini belirleyen bir internet kayıt listesidir. Whois kayıtları, alan adı kaydı ve web sitesi sahiplik sürecinin bütünlüğünü korumak için önemli bir kaynaktır; bir alan adıyla ilişkili herhangi bir riski belirlemeye yardımcı olacak bilgileri ortaya çıkarabilirler.

DOSSIER API'LERI

Dossier, güvenlik bilgileri ve olay yönetimi (SIEM) ve güvenlik düzenleme, otomasyon ve yanıt (SOAR) gibi ilgili çözümler arasında bağlantı kurmayı otomatikleştirerek genel deneyimi iyileştiren ve soruşturma ile yanıt verimliliğini artıran API'ler sağlar.

INFOBLOX TEHDIT ARAŞTIRMASINA ÖNCELIKLI ERIŞIM

Dossier, Infoblox Siber İstihbarat Birimi'nden (CIU) tehdit tavsiyeleri, araştırma notları ve takip analist raporları dahil olmak üzere ortaya çıkan tehditler hakkında en son araştırma ve haberlere hızlı erişim sağlar. Ayrıca, bulut tabanlı bir portal olarak analistleriniz ve araştırmacılarınız bu bilgilere çevrimiçi olarak hızlıca başvurmak veya daha kolay paylaşım için PDF olarak indirmek üzere her yerden, her zaman erişebilirler.

TIDE (THREAT INTELLIGENCE VERI DEĞIŞIMI)

TIDE, BloxOne Threat Defense'ın Dossier'in arkasındaki threat intelligence'ı daha da geliştirebilen ve tüm güvenlik yığınının etkinliğini artırabilen bir başka özelliğidir.

Threat intelligence'ın kontrolünü elinize alın ve TIDE'ın seçtiğiniz kaynaklardan threat intelligence'ı otomatik olarak almasını ve normalleştirmesini sağlayın. Dossier, tehdit avcılığı ve araştırması için en uygun threat intelligence karışımınıza anında erişebilir. Ancak TIDE, seçtiğiniz tehdit akışlarını güvenlik yığınındaki diğer çözümlere otomatik olarak dağıtabilir, bu çözümlerin algılama ve diğer yeteneklerini artırabilir ve genel güvenlik yatırımınızdan daha fazla yararlanmanıza yardımcı olabilir.

Kurumsal Merkez
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Sürüm: 20230915v1