McAfee Threat Intelligence Exchange

Hedeflenmiş saldırılara karşı ortak tehdit istihbaratı

McAfee® Threat Intelligence Exchange, istihbaratı uç nokta, ağ geçidi, ağ ve veri merkezi güvenlik çözümleri genelinde gerçek zamanlı olarak çalışır hale getirerek uyarlanabilir tehdit tespitini ve yanıtını mümkün kılar. İçe aktarılan küresel tehdit bilgilerini yerel olarak toplanmış istihbaratla bir araya getirerek anında paylaşan bu sistem, güvenlik çözümlerinizin tek bir çözüm altında çalışmasını sağlar, ortak istihbarat alışverişi yapar ve bunlara göre harekete geçer. McAfee Threat Intelligence Exchange, tehditle karşılaşma ile hatanın yayılmasını sınırlama arasındaki boşluğun günler, haftalar ve hatta aylardan milisaniyelere indirilmesini sağlar.

İşbirliğine dayalı bir tehdit istihbaratı ekosistemi yaratın

McAfee Threat Intelligence Exchange, bilgi paylaşmak ve entegre güvenlik sağlamak üzere McAfee Data Exchange Layer üzerinden iletilir. Birden fazla tehdit bilgi kaynağından gelen ve bir araya getirilen girişler, üçüncü taraf çözümleri de dahil olmak üzere tüm bağlantılı güvenlik çözümlerinizle paylaşılır.

Güvenlik bileşenleri tek bir sistem gibi çalıştığında, tehdit tespiti ve korumasına destek olan ilgili istihbarat, uç nokta, ağ geçidi, veri merkezi, bulut ve çevrenizdeki diğer güvenlik kontrolü noktaları ile anında paylaşılır. McAfee Data Exchange Layer tarafından sağlanan entegrasyon sadeliği, uygulama ve operasyon maliyetlerini önemli ölçüde azaltırken benzersiz güvenlik, operasyonel verimlilik ve etkinlik sunar.

Tehditlere Karşı Uyum Geliştirebilme ve Bağışıklık Kazanımı

Ağınızdaki her konumdan tespit edilen ve paylaşılan bilgi, hedeflenmiş saldırılara karşı mücadelede yoğun bir farkındalık elde edilmesini sağlar. Bu tehditler tasarımları itibariyle özellikle saldırılara odaklanmış olduğundan, kuruluşlar trendleri ve karşılaştıkları benzersiz atakları yakalamak için Threat Intelligence Exchange (TIE) yerel denetim sistemine ihtiyaç duyarlar. Bu karşılaşmadan toplanan yerel veriler, küresel tehdit istihbaratı servisleri ile de çalıştığından, organizasyonlara daha önce görülmemiş dosyalara karşı daha iyi karar verme olanağı sağlar, koruma ve tespitin eylemlerinin daha hızlı yapılmasını mümkün kılar.

Önemli Avantajları

- Uyarlanabilir tehdit koruması, ileri düzey hedeflenmiş saldırılarla karşılaşma ile hatanın yayılmasını sınırlama arasındaki boşluğu günler haftalar ve hatta aylardan milisaniyelere indirir.
- İşbirliğine dayalı tehdit istihbaratı, küresel istihbarat veri kaynakları ile yerel olarak toplanan tehdit istihbaratının birleşiminden oluşur.
- İlgili güvenlik istihbaratı uç nokta, ağ geçidi, ağ ve veri merkezi güvenlik çözümlerinde gerçek zamanlı olarak paylaşılır.
- Kolektif tehdit istihbaratı ile bir araya gelen uç nokta bağlamına göre (dosya, işlem, ve çevresel özellikler), daha önce hiç görülmemiş dosyalara ilişkin kararlar verme gücüne sahip olursunuz.
- Entegrasyon, McAfee Data Exchange Layer sayesinde daha basit hale getirilir. Tehdit istihbaratınızı gerçek zamanlı olarak çalıştırmak için dışı güvenlik çözümlerinin birbirine bağlanmasıyla uygulama ve operasyon maliyetleri azaltılır.

Bizimle iletişime geçin

Ağınızın herhangi bir noktasında tanımlanamayan bir dosya ile karşılaşıldığında McAfee Threat Intelligence Exchange ile bağlantı kurularak dosya ile ilgili bir istihbarat olup olmadığına bakılır. Bu esnada organizasyondaki yaygınlık ve yayılım yaşı gibi tanımlayıcı meta bilgileri de kolektif istihbarat zekası havuzunda yansıtılır. Entegre güvenlik çözümleri, istihbarat talep etmenin yanı sıra, McAfee Threat Intelligence'da yerel olarak saklanan istihbaratın güncellenmesinde katkıda bulunur. Güncel istihbarat bilgilerinin daha sonra tüm sistemlerinize gerçek zamanlı olarak yayılması sağlanır. Bu yerel tehdit bilgileri gelecek karşılaşmalar için saklanır, yani tehdit daha sonra başka bir cihaz veya sunucuda tekrar görülürse bu kez bilinmeyen bir dosya olmayıp derhal tespiti sağlanacaktır.

McAfee Threat Intelligence Exchange yöneticilerin bu tehdit istihbaratını kolayca şekillendirmelerine olanak tanımaktadır. Koruma sistemini kendi ortam ve şirketlerine özel hale getirebilmeleri için güvenlik yöneticilerine kapsamlı istihbarat bilgilerini **birleştirme**, **geçersiz kılma**, **indirgeme** ve **ayarlama gücü** sunulmaktadır. Yerel olarak önceliklendirilmiş ve ayarlanmış bu tehdit bilgileri, gelecekte yaşanabilecek herhangi bir karşılaşmada anında yanıt imkanı sunmaktadır.

Uygulama Noktaları Korumayı Genişletir

Uç noktadan ağ sınırına kadar ağ geneline entegre olmuş entegre çözümler, mevcut istihbarat, metadata veya data noktaları kombinasyonu baz alınarak politikalar uygulamaktadır. Sıkıca entegre edilmiş yekpare bir çözüm olan McAfee Endpoint Security, birleşimli yerel istihbaratları (organizasyondaki yaygınlık ve yayılım yaşı gibi dosya metadataları ve diğer güvenlik bileşenlerinden alınan lokal istihbaratı) ve mevcut global tehdit istihbaratlarını kullanarak doğru kararlar alabilmektedir. Örneğin, global repütasyonu olmayıp yüksek bir organizasyonel yaygınlığa sahip özel bir uygulama, kötü niyetli kompozit repütasyon oluşturmaz ve muhtelemen çalışmasına izin verilir. Diğer yandan, global veya lokal repütasyona sahip olmayan ve şirkette daha önce görülmemiş bir dosya muhtemelen düşük güven düzeyi oluşturacak, engellemeye maruz kalacak veya McAfee Endpoint Security motorları yoluyla daha ileri incelemeye ihtiyaç duyulacak veya McAfee Advanced Threat Defense ya da McAfee Cloud Threat Detection vasıtasıyla sandboxing işlemine sokulacaktır.

McAfee Endpoint Security'nin makine öğrenim becerisi olan Real Protect ve Dynamic Application Containment ise endpoint denetimi ve korumasını daha geniş bir kapsama yaymaktadır. Real Protect, uygulama öncesi ve sonrası analiz içeren en güncel tehdit istihbaratı ile bulut tarama işlemi gerçekleştirirken, Dynamic Application Containment ek analizler gerçekleştirilirken, endpoint üzerinde kötü amaçlı aktiviteleri engelleyerek yeni bir tehdide maruz kalmış olan ilk makineyi korur.

Önemli Avantajları

Tespit edilmeyi önlemek ve yüksek değere sahip verileri elde etmek için kuruluşta sabit bir zemin bulmak üzere tasarlanmış ileri düzey hedeflenmiş saldırılar, kuruluşların başına bela olmaya devam ediyor. Verizon 2015 Data Breach and Investigations Report kapsamında kısa süre önce yayınlanan verilere göre, kötü amaçlı yazılım örneklerinin %70 ila %90'ı tek bir kuruluşa özel yapıya sahip. Bu da, günümüzün en büyük zorluğunun benzersiz tehdit göstergelerinin tespiti olduğunu gösteriyor.

Daha fazla bilgi için şu adresi ziyaret edin: mcafee.com/TIE.

İşbirliğinden Fayda Sağlayın

Gelişmiş tehdit analizi

Bir dosya hakkında daha fazla bilgi gerekirse, potansiyel yeni tehditlere ilişkin anında ek bilgi edinmek için dosya McAfee Threat Intelligence Exchange'den McAfee Advanced Threat Defense'e gönderilebilir. Bu iki özellik, söz konusu dosyanın bilinirliğini belirlemek için statik ve dinamik kod analizinden elde edilen tehdit analizlerinden faydalanır. Tüm bu işlemler, güvenlik ekosisteminizin tamamını korumak üzere otomatik hale getirilir, belgelenir ve McAfee Data Exchange Layer üzerinden paylaşılır.

Güvenlik olay yönetimi

McAfee Enterprise Security Manager, McAfee Threat Intelligence Exchange tarafından tanımlanan IoC'leri araştırırken daha derinlemesine inceleme yapmanızı mümkün kılar. Geçmiş güvenlik bilgilerine erişim ve otomatik bir takip listesi oluşturma becerisi, kuruluşların güvenlik verimliliğini arttırır.