APT Güvenliği (Sandbox)

McAfee Gelişmiş Tehdit Savunması (Advanced Threat Defense-ATD)

McAfee Gelişmiş Tehdit Savunması (Advanced Threat Defense-ATD) yenilikçi, katmanlı bir yaklaşımla günümüzün gizli, sıfırıncı gün kötü amaçlı yazılımlarını algılar. Çevredeki gelişmiş kötü amaçlı yazılımları bulmak, ağdaki tehdidi dondurmak ve ihlali uç noktada düzeltmek için McAfee ağ güvenliği ve gerçek zamanlı çözümlerle entegre olur.

Çok Kiracılı, Uygulama Programlama Arabirimi (Application Programming Interface-API)

McAfee Advanced Threat Defense, ölçeklenebilir, otomatik ilke yönetimi ve müşteri başına raporlama sağlamak için çok kiracılı, çok etki alanlı McAfee Network Security Manager ve dağıtılmış McAfee Web Gateway (Web Proxy) ürünlerimizle kolayca devreye girer ve entegre olur. Veya şirketinizin kendi merkezi sistemlerinden yönetmek, raporlamak ve faturalandırmak için temsili durum aktarımı (REST) tabanlı API'lere erişin.

Gelişmiş Kötü Amaçlı Yazılım Koruması

McAfee Advanced Threat Defense, geleneksel, imza tabanlı savunmaların ötesine geçer. Kötü amaçlı yazılımın gerçek davranışını analiz etmek için az temaslı anti virüs imzalarını, itibarı ve gerçek zamanlı öykünmeyi derinlemesine statik kod ve dinamik kötü amaçlı yazılım analizi (korumalı alan) ile birleştirir.

Gelişmiş Performans Yönetimi

Bir cihaz, birden çok McAfee ağ güvenlik cihazı, müşteri etki alanı ve hizmetinde günde 250.000'e kadar nesneyi destekleyebilir. Bu, piyasadaki karşılaştırılabilir çözümlerden daha iyi ölçeklenebilir performansla hızlı hizmet sunumuna olanak tanır.

Birleştirilmiş ve Uygun Maliyet

Tek bir cihaz, birkaç farklı analiz çözümünün hizmetlerini değiştirebilir ve birleştirebilir. Bu birleştirilmiş hizmetleri birden fazla müşteriye daha düşük operasyonel maliyetle ölçeklendirerek ve aylık satın alma seçeneğimizi kullanarak daha iyi marjlarda rekabetçi fiyat noktaları sunabilirsiniz.

McAfee Advanced Threat Defense kötü amaçlı yazılımları ortaya çıkarmak için dosya itibarı ve imzalar gibi düşük yoğunluklu yöntemlerden kötü amaçlı yazılım davranışını analiz etmek için dinamik analiz gibi daha karmaşık yöntemlere ve örnekleri sınıflandırmaya yardımcı olmak için derinlemesine statik kod analizine kadar çeşitli analiz teknikleri kullanır. McAfee Advanced Threat Defense, ortaya çıkan tehditleri belirlemek için koddaki kalıpları ortaya çıkarmaya, kötü niyetliliği belirlemek için davranış kalıplarını analiz etmeye ve diğer kötü amaçlı yazılım ailelerine benzerliği belirlemek için kodu değerlendirmeye yardımcı olmak için makine öğrenimini de kullanır.

McAfee Ürünleriyle Birlikte Çalışabilirlik

McAfee Advanced Threat Defense, şu anda McAfee Network Security Platform, McAfee Web Gateway ve McAfee Threat Intelligence Exchange olmak üzere McAfee güvenlik portföyündeki birden çok ürünle entegre olur. McAfee ® Application Control, McAfee ® Endpoint Security çözümleri, McAfee ® Server Security Suite ve McAfee ® Security for Microsoft Exchange ile McAfee Threat Intelligence Exchange entegrasyonları birlikte çalışabilirliği daha da genişletir. Bu vektörlerden kötü amaçlı yazılım örneklerini alan McAfee Advanced Threat Defense, daha sonra kullanılabilir tehdit verilerine ulaşmak için korumalı alan analizi yeteneklerini uygular.

McAfee teknolojileriyle entegrasyona ek olarak, McAfee Advanced Threat Defense, e-posta ağ geçitleri gibi üçüncü taraf güvenlik araçlarıyla da uyumludur. SMTP trafiği, Cisco ESA ve Proofpoint gibi herhangi bir güvenli e-posta ağ geçidine iletilebilir ve bu e-posta ağ geçitleri, bir e-posta ekini analiz için McAfee Advanced Threat Defense'e iletebilir.

Ağ sistemleri, McAfee Advanced Threat Defense, açık kaynaklı Bro Network Security Monitor (bro.org) ile çalışabilir. Bro, bir izinsiz giriş tespit sistemi (IDS) olmasına ve McAfee Network Security Platform gibi sağlam bir izinsiz giriş önleme sisteminin (IPS) yerine geçmemesine rağmen, Bro sensörleri genellikle SOC'ler tarafından kullanılır ve şüpheli bir ağ kesimine izleme amacıyla geçici bir IDS olarak dağıtılır. Bro, dosyaları ağ trafiğinden ayırır ve bir dosya dizinine yerleştirir. McAfee Advanced Threat Defense bu dizinle bütünleşir ve bu dosyaları okuyabilir. Bro, ağ trafiğinden milisaniyeler içinde otomatik olarak bir dosya ayıklayabilen komut dosyaları kullanır ve bir Python komut dosyası ve McAfee Advanced Threat Defense

REST arka plan programı aracılığıyla Bro, dosyayı McAfee Advanced Threat'e gönderir.

McAfee Advanced Threat Defense, araştırmaları destekleyebilecek çok sayıda gelişmiş yetenek sunar:

- Uç nokta, sunucular ve mobil cihazlar için en yaygın kullanılan işletim sistemlerini kapsayan kapsamlı işletim sistemi desteği,
- Derleme çıktısı, ağ paketi yakalamaları (pcaps), grafiksel işlev çağrısı diyagramları ve bellek dökümleri gibi araştırma için kritik bilgiler sağlayan ayrıntılı raporlar,
- Analistlerin ve tehdit avcılarının kötü amaçlı yazılım örnekleriyle doğrudan etkileşim kurmasını sağlayan kullanıcı etkileşimli modu,
- Tipik korumalı alan ortamlarında hareketsiz kalan ek yürütme yollarını zorlayarak daha derin örnek analizi,
- Dosya yürütme için hangi ortam değişkenlerinin gerekli olduğunu belirleyerek araştırmayı hızlandırmak için birden çok sanal ortama örnek gönderme,
- İnceleme süresini günlerden dakikalara indiren kapsamlı paket açma özellikleri.

Analiz için Savunma

Potansiyel olarak kötü amaçlı trafiğe ikinci kez bakmak için daha fazla ağ sensörü kullanarak, araştırmacılarınız gerçek bir pozitiflik elde ettikleri konusunda daha fazla güven kazanabilirler. Ayrıca SOC ekibinize tehdit davranışını daha iyi anlamasını ve ağınızda neler olup bittiğine dair daha derin bir analiz sağlar.

Daha Derin, Daha Doğru Araştırmaları Destekleyen Özellikler

X Modu veya Etkileşimli Mod

Hem avcılar hem de analistler, meşru uygulamalarda geri adım atan tehditler hakkında faydalı ipuçları bulmak için McAfee Advanced Threat Defense X-Mode'dan veya Etkileşimli Moddan yararlanabilir. Bu, özellikle gelişmiş kalıcı tehditlerin (APT'ler) hedefi olan büyük kuruluşlar için geçerlidir.

Keşif görevlerinin bir sonucu olarak, kötü aktörler, hedeflenen kuruluş tarafından günlük olarak kullanılan beyaz listeye alınmış uygulamalar hakkında bilgi edinir. Bilinen bir beyaz listeye alınmış uygulamanın koduna sarılmış tehditler oluştururlar ve keylogger'lar gibi kötü niyetli yükleri yerleştirirler. Kullanıcı tehdidi göremez. Ancak arka uçta, analistiniz veya tehdit avcınız, sürekli olarak anormal veya kötü amaçlı etkinlik arayan McAfee Advance Threat Defense sanal alanındaki kötü amaçlı kodla etkileşime girerse, kötü amaçlı etkinliği belirleyecektir. Şüpheli bir dosya yüklendikten sonra, analist örnekle etkileşime geçebilir ve kullanıcının gerçekte ne göreceğini gördüğü için kullanıcı deneyimini daha iyi anlayabilir. Örneğin, yalıtılmış bir sanal alan içinde, analistiniz beyaz listeye alınmış uygulamanın özelliklerini tıklatabilir ve gömülü bir makro çalıştırmak gibi çeşitli işlemleri yürütebilir. Analistleriniz ve tehdit avcılarınız artık ağınızdaki diğer varlıklara yanal yayılma ve zarar verme endişesi duymadan daha derin manuel araştırma yapma özgürlüğüne sahip.

Benzersiz İşletim Sisteminiz için Özelleştirin

Kullanıcı etkinliğine, yetkilendirilmiş uygulamalara ve kullanımdaki baskın işletim sistemine dayalı olarak belirli bir kuruluşu hedef alan tehditler, birçok işletme için baskın bir odak noktası haline geldi. Kötü amaçlı yazılım yazarı, örneğin, bir işletmenin kullandığı belirli Microsoft Windows işletim sistemi sürümünü biliyorsa, kötü amaçlı yazılımı optimize etmek ve onu olabildiğince zarar verici hale getirmek için bu bilgilerden yararlanabilir, ancak tamamen farklı bir işletim sisteminde çalışan kötü amaçlı yazılımdan daha az belirgindir. Ayrıca, mümkün olduğu kadar çok sisteme sızmak için kötü amaçlı yazılımı çeşitli işletim sistemi sürümlerine göre uyarlayabilirler.

Analistlerin ve tehdit avcılarının bu APT'leri izlemesine ve engellemesine yardımcı olacak başka bir mekanizma, McAfee Advanced Threat Defense'de analiz ortamını özelleştirme yeteneğidir. Belirli bir işletim sistemi sürümü veya belirli uygulamalarla bir ortamdaki olası tehditleri analiz edebilirsiniz. Kötü amaçlı yazılım örnekleri daha sonra özelleştirilmiş analiz VM'lerinde güvenli bir şekilde patlatılabilir. Bu, kendi ortamınızı yansıttığı ve ekibinizin iyileştirme sürecini hızlandıracak ve etkinliğini en üst düzeye çıkaracak IoC'leri çıkarmasına yardımcı olduğu için tehdit avlama çabalarınız için büyük bir kazançtır.

Paylaşın ve Yayınlayın

McAfee Advanced Threat Defense, çeşitli yöntemler kullanılarak yapılan titiz bir analizden sonra IoC'lerini ve kanaatlerini paylaşabilir. Çıktılar, demontaj, işlev çağrısı diyagramları, bırakılan dosya ayrıntıları, işlemler ve kayıt defteri değişiklikleri gibi kritik araştırma bilgilerini içerir. McAfee Advanced Threat Defense, meta verileri ve sonuçları tehdit istihbarat platformları, makine veri analizi çözümleri ve SIEM'lerle paylaşan yayıncı olur.

Savunma, tehdit istihbaratını McAfee Tehdit İstihbarat Borsası'na yayınlayabilir; bu bilgileri tüm güvenlik ekosisteminiz genelinde anında paylaşarak çözümlerinizin (hem McAfee ürünleri hem de uyumlu üçüncü taraf ürünleri) politikalarını uyarlamak için birlikte çalışmasına ve tehditleri daha hızlı bir şekilde ele almasına olanak tanır. uygun koruma ve iyileştirme.

Açık kaynak sürümü olan Açık Veri Değişim Katmanı (OpenDXL), basit açık kaynak araçları, uzmanlık ve destekleyici bir topluluk sağlayarak oyun alanını daha da genişletir. Dahili olarak geliştirilmiş veya satıcı tarafından sağlanan herhangi bir uygulama, DXL iletişim yapısının gerçek zamanlı yeteneklerinden yararlanabilir ve böylece McAfee Advanced Threat Defense tarafından sağlanan zengin tehdit istihbaratı bilgilerinden yararlanabilir.

STIX/ OpenTAXII

McAfee Advanced Threat Defense, siber tehdit istihbaratının paylaşımını sağlayan yaygın olarak kullanılan standartları benimseyerek işbirlikçi bir güvenlik ekosistemi oluşturma, destekleme ve genişletme yeteneğimizi daha da ortaya koyuyor. Bilgileri Açık Kaynak biçiminde, özellikle de Yapılandırılmış Tehdit Bilgi İfadesi (STIX) biçimindeki tehdit bilgilerini, tehdit istihbaratını paylaşmak için bir aktarım mekanizması olan Güvenilir Otomatik Gösterge Bilgisi Değişimi (TAXII) aracılığıyla yayınlar.

Hash'ler, kötü amaçlı IP'ler ve kullanıcı kimlikleri gibi ayrıntılarla IoC'leri kolayca tüketmesine olanak tanır. Bu tür bilgiler, SOC analistlerinin ve tehdit avcılarının bir dosyanın veya eylemin amacını daha net bir şekilde anlamalarını sağlar. STIX/TAXII açık standartları desteği, McAfee Advanced Threat Defense tarafından oluşturulan bilgilerin TAXII'yi destekleyen hemen hemen her SIEM çözümü aracılığıyla ayrıştırılıp ilişkilendirilebilmesi açısından gerçek bir değere sahiptir. Analistler ve tehdit avcıları daha sonra çevrelerinde olup bitenler hakkında hem tarihsel hem de gerçek zamanlı olarak daha bütünsel bir anlayış elde edebilirler.

McAfee'den Zengin ve Kapsamlı Analiz Raporları

Gelişmiş Tehdit Savunması, analistlerin ve tehdit avcılarının hızla harekete geçmesini sağlayan anlamlı veriler sağlar. Bu anlaşılması kolay raporlar, SOC'den C-suite'e kadar tüm kuruluş genelinde değer sağlar.

McAfee Advanced Threat Defense raporunda sunulan en önemli ve faydalı bilgilerden bazıları şunları içerir:

- Davranış sınıflandırması: Kötü amaçlı yazılım sınıflandırmasının bu üst düzey göstergesi, analiz edilen dosyaların amacına ilişkin anında içgörüler sağlayarak analistler ve tehdit avcıları için büyük bir değer sunar.
- Doğrudan MITRE ATT&CK çerçevesine eşleme: MITRE Çelişkili Taktikler, Teknikler ve Ortak Bilgi (ATT&CK™) çerçevesi, analistlerin rakipleri ve çalışmalarını daha iyi anlamalarına yardımcı olabilir. ATT&CK çerçevesini McAfee Advanced Threat Defense'e dahil eden McAfee, analistlerin belirli bir tehdidin tekniklerini, taktiklerini ve prosedürlerini (TTP'ler) daha hızlı anlamasını kolaylaştırdı. Bu bilgilere sahip olduklarında, ilgili savunmaları veya keşif yöntemlerini uygulamak için daha hızlı hareket edebilirler.
- Ayrıntılı bilgiler ve IoC'ler: McAfee Advanced Threat Defense, inceleme için sökme çıktısı, bellek dökümleri, grafiksel işlev çağrısı diyagramları, gömülü veya bırakılan dosya bilgileri, kullanıcı API günlükleri ve PCAP bilgileri dahil olmak üzere derinlemesine tehdit istihbaratı üretir. Tehdit zaman çizelgeleri, saldırı yürütme adımlarının görselleştirilmesine yardımcı olur.

McAfee Advanced Threat Defense, güvenlik operasyonları ekiplerini, analist araştırmalarını ve tehdit avını destekleyebilecek çok sayıda gelişmiş yetenek sunar:

- Uç nokta, sunucular ve mobil cihazlar için en yaygın kullanılan işletim sistemlerini kapsayan kapsamlı işletim sistemi desteği
- Derleme çıktısından, ağ paketinden araştırma için kritik bilgiler sağlayan ayrıntılı raporlar
- Yakalamalar (pcaps), grafiksel işlev çağrı şemaları ve bellek dökümleri
- Analistlerin ve tehdit avcılarının doğrudan kötü amaçlı yazılımlarla etkileşim kurmasını sağlayan kullanıcı etkileşimli mod.