McAfee Active Response

Kapsamlı uç nokta tespiti ve müdahalesi

Günümüzde, güvenlik konusunda bilinçli şirketler çarpıcı bir hızla değişen tehdit ortamı ile karşı karşıyalar. Saldırılar daha önce hiç görülmemiş bir hızda oluşturuluyor ve yayılıyor. "Özel tasarlanmış" saldırılar, etkinliklerini arttırmak ve tespit edilme risklerini en aza indirmek için belirli bir alana odaklanmış bilgiler kullanarak bağımsız kuruluşları hedefliyorlar. Saldırılardan sorumlu olanlar, önleyici teknolojilere daha sık sızmaya başladılar. Bu nedenle ileri görüşlü kuruluşlar, saldırganların varlığını daha iyi tespit eden ve hızlı araştırma ve onarımı mümkün kılan, kullanımı kolay ve entegre araçlar talep ediyor. En iyi tespit ve müdahale çözümleri, sayısı giderek artan sistemlerden her geçen gün daha fazla bilgi toplayarak güvenlik verimliliğini arttırıyor. Üstün ve kullanıma hazır becerileri, mevcut güvenlik yönetimi çözümleri ile otomatik etkileşimi ve kullanıcı özelleştirme özelliğini sunan McAfee® Active Response, saldırganların bilgi işlem varlıklarınıza ve kurumsal markanıza zarar verme fırsatlarını büyük ölçüde daraltıyor.

Evrilen Tehdit Ortamı

Her an bir saldırıya uğrayabileceklerinin farkına varan şirketler, saldırıyı önceden tespit ederek, devam eden aktiviteleri saptayarak veya saldırı göstergelerini (IoA) keşfederek bu ihlallerin etkin şekilde üstesinden gelmeye hazır olmalıdır. Bu gerçek fark edildiğinde, görünürlük, keşif, tespit ve müdahale konularındaki mevcut boşlukların giderilmesi için yeni teknolojilerin gerekli olduğu anlayışı ortaya çıkar.

Mevcut Olaya Müdahale Yaklaşımlarındaki Sınırlamalar

Kuruluş genelinde şüphelenilen veya bilinen bir olayı araştırması istenen olay müdahale ekipleri veya güvenlik yöneticilerinin önünde genelde iki kısıtlayıcı engel bulunur: zaman ve ölçek. Ayrıntılı bilgilerin büyük kısmı mevcut sistemler veya araçlarla toplanıyor olsa da, bu bilgilerin toplanması ve analiz edilmesi uzun zaman alır. Hızın veri toplama açısından çok kritik bir gereklilik olması nedeniyle, toplanan verilerin yapısı ve verilerin toplandığı sistemlerin sayısı açısından önemli tavizler verilir.

Önemli Avantajlar

- **Otomatik:** Saldırı göstergesi (IoA) olabilecek değişiklikleri görmek için bağlamı ve sistemi yakalayın ve izleyin; pasif saldırı bileşenlerini bulun, istihbaratı analiz, operasyon ve adli ekiplere gönderin.
- **Uyarlanabilir:** Uyarı aldığınızda, saldırı metodolojilerindeki değişikliklere uyum sağlayabilir; veri toplama, uyarı, önemli nesnelere yapılan müdahaleler gibi işlemleri otomatik hale getirebilir; yapılandırmanızı müşteri iş akışlarına göre özelleştirebilirsiniz.
- **Daimi:** Israrcı toplayıcılar, saldırı etkinliklerini tespit eder etmez tetiklemeleri etkinleştirerek izlemekte olduğunuz saldırı aktivitesi için sizi ve sistemlerinizi uyarır.

Bizimle iletişime geçin

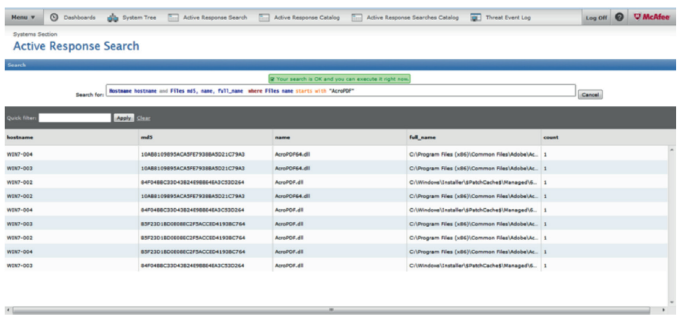
Ayrıca, kilit bilgilerin tanımlanması için ayıklanması gereken toplanmış verilerin büyüklüğü, işleme sürecinin giderek daha da zorlaşmasına neden olur.

En yaygın kullanılan olaya müdahale araçları, müdahale ekipleri tarafından yazılan kodlardır. Veri toplamanın temelini oluşturan bu araçlar, daha geniş analizlerde kullanılır. Bilgi tabanı ve ilgili araçlar büyük ölçüde olgunluğa ulaşmış olsa da, bunları ölçeklenmiş ve hızlı bir şekilde kullanma becerisi kısıtlıdır. Kuruluş genelindeki belirli saldırı göstergelerine yönelik canlı bir araştırma gerçekleştirme becerisinin olmaması, genelde müdahale ekiplerinin keşiflerinde ve müdahale çabalarında ileriyi görememesine neden olur. Tipik olarak zaman gerekliliklerini karşılamak üzere yapay olarak sınırlandırılan bu çabalar, olaya müdahale sürecinde önemli eksikliklere neden olabilir. Bu da, mevcut araçların kısıtlamaları nedeniyle çabaları yapay olarak sınırlandırılan müdahale ekiplerinin önünde engel oluşturur.

Kapsamlı Uç Nokta Tespiti ve Müdahalesi

McAfee Active Response, güvenlik uzmanlarının güvenlik duruşunu izlemesine, tehdit tespitini daha iyi hale getirmesine, ileri görüşlü keşfetme, ayrıntılı analiz, adli araştırma, kapsamlı raporlama yöntemleri ile önceliklendirilmiş uyarılar ve eylemlerle olaya müdahale becerilerini geliştirmesine yardımcı olmak için gelişmiş güvenlik tehditlerinin daimi olarak tespit edilmesini ve bu tehditlere müdahale edilmesini sağlar. Sıkı uç nokta tespit ve müdahale (EDR) kriterlerini karşılamak üzere optimize edilen McAfee Active Response, yalnızca çalıştırma işlemlerinde bulunan değil, aynı zamanda pasif durumda bekleyen veya silinmiş olan saldırı göstergelerini bulmak için tüm sistemler genelinde derinlemesine araştırma yapmak üzere önceden tanımlanmış ve kullanıcı tarafından özelleştirilebilir toplayıcılardan faydalanır. Üstelik kullanıcıların o anda bulunan saldırı göstergelerini aramasının yanı sıra, ileride saldırı göstergelerinin ortaya çıkması durumunda talimat veren tetikleyiciler sayesinde güvenlik hedeflerine uygun uyarılar vermesini ve harekete geçmesini sağlar.

McAfee Active Response, daha fazla tehdidi daha karmaşık bir dünyada, daha hızlı bir şekilde ve daha az kaynak kullanarak çözümlemek üzere tasarlanmış entegre güvenlik mimarisinin ne kadar etkili olduğunun kanıtıdır. McAfee Active Response, uç noktalarınıza yönelik daimi görünürlük ve güçlü görüşler sunarak ihlalleri daha hızlı bir şekilde tespit etmenizi sağlar. Ayrıca, sorunları hızlı ve şirketiniz için en makul şekilde çözmek için ihtiyacınız olan araçları sunar. Tüm gücünü McAfee Data Exchange Layer'dan faydalanan McAfee® ePolicy Orchestrator® (McAfee ePO ™) yazılımından alarak, ürünü uygulayacak personel sayısını arttırmaya gerek kalmadan birleşik ölçeklenebilirlik ve genişletilebilirlik sağlar.



Şekil 1. McAfee Active Response sarch kullanıcı arayüzü.

Sistem Gereksinimleri

Minimum donanım gereklilikleri:
Sunucu, gerektiğinde sanal bir makineye kurulabilir. McAfee Active Response sunucusu için gerekli minimum donanım gereklilikleri şöyledir:

- 4 Intel® Xeon® CPU X5675, 3,07 GHz
- 8 GB RAM
- 120 GB solid state disk

Gerekli hizmet altyapısı

- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.1.1 veya üstü
- McAfee Agent 5.0 uzantısı veya üstü
- McAfee Data Exchange Layer 2.0.0.405 aracısı veya üstü

Desteklenen web tarayıcıları

- Internet Explorer 9 veya üstü
- Chrome 17 veya üstü
- Firefox 10.0 veya üstü

Gerekli istemci altyapısı

- Linux uç noktaları için McAfee Agent 5.0.0.2710 veya üstü
- Microsoft Windows uç noktaları için McAfee Agent 5.0.0.2610 veya üstü
- Tüm yönetimli uç noktalarında McAfee Data Exchange Layer 2.0.0.405 istemcileri veya üstü

BILGI FORMU

Özellik	Avantaj	Müşteri Avantajları	Farklı Yönleri
Toplayıcılar (Collectors)	Toplayıcılar, kullanıcıların sistemlerindeki verileri bulmalarını ve görselleştirmelerini mümkün kılar.	Sistemleri daha derinlemesine incelemeyi sağlayan arama becerileri sunar. Toplayıcılar, bu sistemlerdeki verileri toplamak ve görselleştirmek üzere kritik ihlallere veya saldırı potansiyellerine yönelik görünürlük sağlar. Kullanıcılar, çok sayıdaki ortak kod yazma dillerinden birini kullanarak kendi toplayıcılarını ve müdahalelerini kolaylıkla özelleştirebilir, böylelikle ideal yapılandırılabilirlik ve uyarlanabilirlik sağlarlar.	McAfee Active Response, pasif haldeki, hatta saldırganın arkasında iz bırakmamak için silmeye çalışmış olabileceği kodda çalıştırılabilir veya çalışan dosyaların ötesine bakar. McAfee Active Response, dosya, ağ akışı ve kayıt aramanın yanı sıra eşleştirme de yapabilir.
Tetikleyiciler (Triggers)	Tetikleyiciler, güvenlik uzmanının tek bir talimat kümesi ile hem o anda hem de gelecekte kritik olaydaki veya durumdaki değişimi sürekli olarak izlemesini sağlar.	Önceden belirlenmiş bir tetikleyici ile başlatılan eylemler, bir olay oluşturur veya müdahale gerçekleştirir. McAfee Active Response, durağan "görüşlerin" ötesinde daimi müdahale moduna geçme becerisine sahiptir.	Tehditleri bugün görerek yarın karşılaşabileceğiniz tehditlere yönelik eylemleri tetikleyebilir.
Tepkiler (Reactions)	Tepkiler, tetikleyicinin şartlarını karşılayarak ve tehditleri bulup ortadan kaldırmanızı sağlayarak önceden yapılandırılmış ve özelleştirilebilir eylemler sunar.	Kullanıcıların, sistemden silinen dosyaları sağlama dosyasına (MD5 ve SHA1) göre aramak, ana bilgisayarlardan herhangi birinin geçmişte bir IP adresine aktif olarak bağlanıp bağlanmadığını görmek veya sistemde erişilmemiş veya aktif hale gelmemiş PE dışı kötü amaçlı dosyaları aramak (dosya sistemine kopyalanmış ancak açılmamış kötü amaçlı PDF'i sistemde aramak) gibi eylemleri gerçekleştirmesini sağlar.	McAfee Active Response, arama bulgularına göre hareket edecek ve belirli kullanıcı tanımlı ihtiyaçları karşılamak için kullanıcının belirttiği özel eylemleri gerçekleştirecek şekilde önceden yapılandırılmıştır.
McAfee ePO Yazılımı ile Merkezi Yönetim	Tek konsollu ortam, kapsamlı yönetim ve otomasyon sunar.	Yöneticiler, tetikleyicilere ve aramalara otomatik müdahalede bulunulmasını sağlamak, tehditlere müdahale etmek ve sayılarını azaltmak üzere McAfee ePO yazılımını entegre güvenlik mimarisi olarak kullanabilirler. Ürünün tek bir ekrandan yönetilebilmesi, fazladan idari iş yükü doğurmadan daha fazla güvenlik görünürlüğü sunar. Böylelikle, operasyonel yöntemler sadeleştirilir ve idari personelin harcadığı zaman azaltılır.	Tek bir konsoldan gerçekleştirilen yönetim ve uygulama, ürünü diğerlerinden net olarak ayıran bir özelliktir. Tek bir konsol kullanarak, bir dizi güçlü güvenlik kontrolü ile McAfee Active Response da dahil birçok platformu benzersiz bir şekilde koruyoruz.
Entegre Güvenlik Mimarisi	Entegre güvenliğin parçası olan McAfee'nin diğer ürünleri ile olan iletişimini standartlaştırmak için veri alışverişi katmanından faydalanır.	McAfee'nin entegre güvenlik mimarisinin bir parçası olan McAfee Active Response, platformun inovatif konseptleri, optimize edilmiş süreçleri ve pratik tavsiyeleri ile riski ve yanıt süresini azaltır, genel giderleri ve operasyonel personel maliyetini aşağı çeker.	

Daha Fazlası

Daha fazlası için ziyarat edin.

https://www.banasorun.net/category/mcafee-enterprise/ .

McAfee Together is power.

McAfee çözümlerinin ağınızı gizli ve gelişmiş tehditlere karşı nasıl güvence altına alabileceği hakkında daha fazla bilgi için müşteri temsilcinizle iletişime geçin veya www.banasorun.net/category/mcafee-enterprise/ adresini ziyaret edin.

BANASORUN teknoloji danışmanları