Olay Müdahalesi

Bir güvenlik olayı, dijital varlıkların, ağların, verilerin veya kaynakların gizliliğini, bütünlüğünü veya kullanılabilirliğini riske atan veya tehdit eden herhangi bir olumsuz olay veya faaliyeti ifade eder. Bu tür olaylara yetkisiz erişim, veri ihlalleri, kötü amaçlı yazılım enfeksiyonları, hizmet reddi saldırıları ve bir kuruluşun bilgi teknolojisi ortamının güvenlik duruşunu tehlikeye atan diğer tüm faaliyetler dahildir.

Olay müdahalesinin amacı, bir güvenlik olayını etkili bir şekilde ele almak ve normal iş operasyonlarını mümkün olan en kısa sürede geri yüklemektir. Kuruluşların dijital varlıkları sürekli büyüdükçe, olayları manuel olarak yönetmek giderek daha zor hale gelir, dolayısıyla otomasyona ihtiyaç duyulur.

Otomatik olay müdahalesi, güvenlik olaylarına müdahale ederken gerçekleştirilen otomatik eylemleri içerir. Bu eylemler, tehlikeye atılmış uç noktaları izole etmeyi, kötü amaçlı IP adreslerini engellemeyi, enfekte cihazları karantinaya almayı veya tehlikeye atılmış kullanıcı hesaplarını devre dışı bırakmayı içerebilir. Olay müdahalesini otomatikleştirerek, siber güvenlik ekipleri tespit edilen tehditlere verilen yanıt süresini azaltır, olayların etkisini önler veya en aza indirir ve büyük miktarda güvenlik olayını verimli bir şekilde yönetir.

Wazuh Aktif Tepki modülü

Wazuh Aktif Tepki modülü, kullanıcıların uç noktalarda olaylar algılandığında otomatik eylemler yürütmesine olanak tanır. Bu, bir organizasyonun olay yanıtlama süreçlerini iyileştirerek güvenlik ekiplerinin algılanan tehditlere karşı anında ve otomatik eylemler gerçekleştirmesini sağlar.

Eylemleri durumsuz veya durumlu olacak şekilde de yapılandırabilirsiniz. Durumsuz etkin yanıtlar tek seferlik eylemlerdir, durumlu yanıtlar ise bir süre sonra eylemlerini geri alır.

Varsayılan Etkin Yanıt Eylemleri

Wazuh aracılarını çalıştıran her işletim sisteminde kullanıma hazır betikler mevcuttur. Varsayılan etkin yanıt betiklerinden bazıları şunlardır:

Komut dosyası adı	Tanım

hesabı devre dışı bırak	Bir kullanıcı hesabını devre dışı bırakır
güvenlik duvarı-bırakma	Iptables reddetme listesine bir IP adresi ekler.
güvenlik duvarıd-bırak	Güvenlik duvarının bırakma listesine bir IP adresi ekler.
yeniden başlat.sh	Wazuh aracısını veya sunucusunu yeniden başlatır.
netsh.exe	Netsh kullanarak bir IP adresini engeller.

Özel etkin yanıt eylemleri

Wazuh Active Response modülünün faydalarından biri de uyarlanabilirliğidir. Wazuh, güvenlik ekiplerinin herhangi bir programlama dilinde özel aktif yanıt eylemleri oluşturmasına ve bunları kendi özel ihtiyaçlarına göre uyarlamasına olanak tanır. Bu, bir tehdit algılandığında yanıtın kuruluşun gereksinimleriyle uyumlu olacak şekilde özelleştirilebilmesini sağlar.

Wazuh ile olay müdahalesini otomatikleştirme

Wazuh Active Response modülünden yararlanmak için, izlenen bir uç noktada belirli bir olay meydana geldiğinde gerçekleştirilecek eylemi yapılandırmanız gerekir . Örneğin, Wazuh Active Response modülünü enfekte bir uç noktadan kötü amaçlı bir yürütülebilir dosyayı silecek şekilde yapılandırabilirsiniz. Aşağıdaki örneklerde, Wazuh Active Response modülünün farklı olayları nasıl ele aldığını gösteriyoruz.

Kötü amaçlı yazılımları kaldırma

Kötü amaçlı dosyaları bir uç noktadan tespit etmek ve kaldırmak için Wazuh Active Response modülünü Dosya Bütünlüğü İzleme modülü ve VirusTotal entegrasyonuyla birlikte kullanabilirsiniz .

Aşağıdaki görselde şu aktiviteler gösterilmektedir:

1. Wazuh Dosya Bütünlüğü İzleme modülü ile izlenen dizine `554`bir dosya eklendiğinde Kural Kimliği tetiklenir.`Downloads`
2. Kural Kimliği, `87105`Wazuh dosya karmasını çıkardığında, API'si aracılığıyla VirusTotal veritabanından dosya karması hakkında veri istediğinde ve kötü amaçlı bir dosya yanıtı aldığında tetiklenir.
3. Wazuh Dosya Bütünlüğü İzleme modülü ile izlenen dizinden `553`bir dosya silindiğinde Kural Kimliği tetiklenir.`Downloads`

4. Kural Kimliği, `110006`Wazuh Active Response modülü kötü amaçlı dosyayı uç noktadan sildiğinde tetiklenir.

Kötü amaçlı yazılım etkinlik olaylarını kaldırma



Bu senaryoda, Wazuh Active Response modülü kötü amaçlı dosyayı otomatik olarak kaldırarak tehdit tespiti ile azaltma arasındaki süreyi kısaltır.

DoS saldırılarına yanıt verme

Bir DoS saldırısının birincil amacı, hedefi meşru kullanıcılar için erişilemez hale getirerek hizmet reddi oluşturmaktır. Aşağıdaki görüntüde, Wazuh Active Response modülünün Ubuntu uç noktasındaki bir web sunucusuna karşı DoS gerçekleştiren kötü amaçlı IP adreslerini nasıl engellediğini gösteriyoruz.

Ana bilgisayar Active Response uyarıları tarafından engellendi



Bu durumda, Wazuh Active Response modülü kötü niyetli ana bilgisayarların web sunucusunda bir DoS saldırısı düzenlemesini otomatik olarak engeller. Böylece web sunucusunun yetkili kullanıcılar için kullanılabilirliği garanti altına alınır.

Kaba kuvvet saldırısından sonra bir kullanıcı hesabını devre dışı bırakma

Hesap kilitleme, bir kullanıcının belirli bir zaman diliminde yapabileceği oturum açma girişimi sayısını sınırlayarak kaba kuvvet saldırılarına karşı savunmak için kullanılan bir güvenlik önlemidir. Parolası bir saldırgan tarafından tahmin edilen kullanıcı hesabını devre dışı bırakmak için Wazuh Active Response modülünü kullanırız.

Aşağıdaki görselde Wazuh Active Response modülü, Linux uç noktasındaki hesabı devre dışı bırakıyor ve 5 dakika sonra tekrar etkinleştiriyor.

Linux hesabı geçici olarak devre dışı bırakıldı uyarıları



Bu senaryoda, bir saldırgan bir kullanıcının parolasını tekrar tekrar tahmin etmeye çalıştığında ve başarısız olduğunda, hesap geçici olarak erişilemez hale gelir. Bu, kullanıcı hesabı parolalarını tahmin etmek için kaba kuvvet yöntemlerine güvenen saldırganların işini engeller.

Wazuh Active Response modülünü kullanarak güvenlik ekipleri farklı olaylara verilen yanıtları otomatikleştirebilir. Böylece etkili olay yanıtı ve daha dayanıklı bir siber güvenlik duruşu sağlanabilir.

Revision #7
Created 6 December 2023 18:02:22 by LastGuard

Updated 11 December 2024 22:18:26 by Ayşegül Sarıkaya