Aktif Tepki

Güvenlik ekipleri, yüksek öneme sahip olayları zamanında ele almak veya tam azaltma eylemleri sağlamak gibi olay yanıtlarında sıklıkla sorunlarla karşılaşırlar. Gerçek zamanlı olarak ilgili bilgileri toplamakta zorlanabilirler, bu da bir olayın tam kapsamını anlamayı zorlaştırır. Bu sorunlar, bir siber saldırının etkisini sınırlama ve azaltma zorluğunu artırır.

Wazuh SIEM ve XDR platformu, olaylara müdahaleyi şu şekilde iyileştirir:

- Güvenlik olaylarına ilişkin gerçek zamanlı görünürlük sağlamak.
- Uyarı yorgunluğunun azaltılması.
- Tehditlere karşı yanıt eylemlerinin otomatikleştirilmesi.
- Hazır yanıt senaryoları sağlamak.

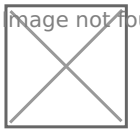
Wazuh, güvenlik ekiplerinin belirli tetikleyicilere dayalı yanıt eylemlerini otomatikleştirmesine yardımcı olan ve güvenlik olaylarını etkili bir şekilde yönetmelerini sağlayan bir Active Response modülüne sahiptir.

Yanıt eylemlerinin otomatikleştirilmesi, yüksek öncelikli olayların zamanında ve tutarlı bir şekilde ele alınmasını ve düzeltilmesini sağlar. Bu, özellikle güvenlik ekiplerinin kaynaklarının kısıtlı olduğu ve yanıt çabalarını önceliklendirmeleri gereken ortamlarda değerlidir.

Ek olarak, modül tehditlere yanıt vermeye ve bunları azaltmaya yardımcı olan bir dizi kullanıma hazır yanıt betiği içerir. Örneğin, bazı betikler kötü amaçlı ağ erişimini engeller ve izlenen uç noktalardaki kötü amaçlı dosyaları siler. Bu eylemler güvenlik ekiplerinin iş yükünü azaltır ve olayları etkili bir şekilde yönetmelerini sağlar.

Wazuh Active Response modülü, belirli bir kural kimliği, seviyesi veya kural grubu uyarısı tetiklendiğinde izlenen uç noktalarda bu betikleri yürütür. Bir tetikleyiciye yanıt olarak başlatılacak herhangi bir sayıda betik ayarlayabilirsiniz; ancak bu yanıtları dikkatlice değerlendirmelisiniz. Kuralların ve yanıtların kötü uygulanması, bir uç noktanın savunmasızlığını artırabilir.

Aşağıdaki görsel Active Response iş akışını göstermektedir.



Aktif yanıt türleri

Aktif bir yanıt şunlardan biri olabilir:

- Vatansız
- Durum bilgisi

Durumsuz etkin yanıtlar, onları geri döndürmek veya durdurmak için bir olay tanımı olmayan tek seferlik eylemlerdir. Durumlu yanıtlar, eylemlerini bir süre sonra geri döndürür veya durdurur.

Revision #2
Created 11 December 2024 19:10:31 by Ayşegül Sarıkaya
Updated 31 December 2024 17:57:35 by Ayşegül Sarıkaya