Güvenlik Yapılandırma Değerlendirmesi

Güvenlik Yapılandırma Değerlendirmesi (SCA), tüm sistemlerin yapılandırma ayarları ve onaylı uygulama kullanımıyla ilgili önceden tanımlanmış bir dizi kurala uyduğunu doğrulama sürecidir. Uç noktaları güvence altına almanın en kesin yollarından biri, güvenlik açığı yüzeylerini azaltmaktır. Bu süreç genellikle güçlendirme olarak bilinir. Yapılandırma değerlendirmesi, uç noktalarınızdaki zayıflıkları belirlemenin ve saldırı yüzeyinizi azaltmak için bunları yamamanın etkili bir yoludur.

Wazuh SCA modülü, izlenen uç noktalardaki yanlış yapılandırmaları ve ifşaları tespit etmek ve düzeltme eylemleri önermek için taramalar gerçekleştirir. Bu taramalar, uç noktaların yapılandırmasını, uç noktanın gerçek yapılandırmasına karşı test edilecek kuralları içeren politika dosyalarını kullanarak değerlendirir. SCA politikaları, dosyaların, dizinlerin, kayıt defteri anahtarlarının ve değerlerinin, çalışan işlemlerin varlığını kontrol edebilir ve dizinlerin içindeki dosyaların varlığını yinelemeli olarak test edebilir.

Örneğin, SCA modülü parola ile ilgili yapılandırmanın değiştirilmesinin, gereksiz yazılımların kaldırılmasının, gereksiz hizmetlerin devre dışı bırakılmasının veya TCP/IP yığın yapılandırmasının denetlenmesinin gerekli olup olmadığını değerlendirebilir.

SCA modülü için politikalar YAML'de yazılmıştır. Bu format, insan tarafından okunabilir ve anlaşılması kolay olduğu için seçilmiştir. Kendi SCA politikalarınızı kolayca yazabilir veya mevcut olanları ihtiyaçlarınıza uyacak şekilde genişletebilirsiniz. Ayrıca, Wazuh çoğunlukla uç nokta güçlendirme için yerleşik bir standart olan CIS kıyaslamalarına dayalı bir dizi kullanıma hazır politika ile dağıtılır.

Revision #2
Created 23 December 2024 19:20:17 by Ayşegül Sarıkaya
Updated 31 December 2024 17:59:12 by Ayşegül Sarıkaya