Ajansız İzleme

Wazuh sunucusu, uç noktalardaki güvenlik olaylarını ve vakalarını izlemek, tespit etmek ve bunlara ilişkin uyarıları tetiklemek için Wazuh ajanlarından aldığı verileri analiz eder. Ancak bazı uç noktalarda Wazuh ajanının kurulumunu engelleyen sınırlamalar olabilir. Wazuh, ajansız izleme yeteneğini kullanarak bu sorunu çözer.

Aracısız izleme, bir aracı veya yazılım yüklemeyi gerektirmeyen bir uç nokta izleme türünü ifade eder. Bu yaklaşım, izlenen uç noktadan bilgi edinmek ve toplamak için mevcut protokolleri kullanır.

Wazuh ajansız izleme yeteneği, olayları uç noktalardan Wazuh sunucusuna toplamak ve aktarmak için SSH (Güvenli Kabuk) protokolünü kullanır. Desteklenen platformlar arasında yönlendiriciler, güvenlik duvarları, anahtarlar ve Linux/BSD sistemleri bulunur. Yazılım yükleme kısıtlamaları olan uç noktaların güvenlik ve uyumluluk gereksinimlerini karşılamasını sağlar.

Revision #2
Created 11 December 2024 16:24:40 by Ayşegül Sarıkaya
Updated 31 December 2024 18:00:27 by Ayşegül Sarıkaya