Sistem Envanteri

Sistem envanteri, bir BT altyapısındaki donanım ve yazılım varlıkları hakkında bilgi içeren bir kaynaktır. Tüm varlıkların envanterini tutmak, kuruluşların ortamlarındaki donanım ve yazılım görünürlüğünü en üst düzeye çıkarmalarına yardımcı olur. Güncel bir sistem envanteri, bir kurumsal ağ içinde iyi bir BT hijyeni sağlamak için olmazsa olmazdır.

Merkezi bir sistem envanteri tutmak için Wazuh aracıları izlenen uç noktalardan sistem bilgilerini toplar ve bunları Wazuh sunucusuna gönderir. Wazuh Syscollector modülü, bu tür verileri her bir aracıdan toplamaktan sorumludur. Wazuh aracısının topladığı veriler arasında donanım ve işletim sistemi bilgileri, yüklü yazılım ayrıntıları, ağ arayüzleri, bağlantı noktaları ve çalışan işlemler bulunur. Wazuh aracısı ayrıca Windows uç noktalarından Windows güncelleştirmeleri hakkında veri toplayabilir. Syscollector modülünün ne tür bilgileri toplamasını veya yoksaymasını istediğinizi yapılandırabilirsiniz.

Kullanıcılar, tehdit avı ve BT hijyeni egzersizleri sırasında değerli kaynaklar olabilecek Wazuh panosundan sistem envanter raporları oluşturabilir. Raporda yer alan bilgiler, istenmeyen uygulamaları, süreçleri, hizmetleri ve kötü amaçlı eserleri tanımlamak için kullanılabilir.

Revision #2
Created 11 December 2024 20:48:09 by Ayşegül Sarıkaya
Updated 31 December 2024 17:59:47 by Ayşegül Sarıkaya