Günlük Veri Toplama

Günlük veri toplama, bir ağ içindeki farklı günlük kaynaklarından günlükleri toplamayı ve birleştirmeyi içerir. Günlük veri toplama, güvenlik ekiplerinin düzenleyici uyumluluğu karşılamalarına, tehditleri tespit edip düzeltmelerine ve uygulama hatalarını ve diğer güvenlik sorunlarını belirlemelerine yardımcı olur.

Wazuh, uç noktalardan, ağ aygıtlarından ve uygulamalardan günlükleri toplar, analiz eder ve depolar. İzlenen bir uç noktada çalışan Wazuh aracısı, analiz için sistem ve uygulama günlüklerini toplar ve Wazuh sunucusuna iletir. Ayrıca, syslog veya üçüncü taraf API entegrasyonları aracılığıyla günlük mesajlarını Wazuh sunucusuna gönderebilirsiniz.

Revision #2
Created 11 December 2024 16:22:20 by Ayşegül Sarıkaya
Updated 31 December 2024 17:57:53 by Ayşegül Sarıkaya