Komut İzleme

Wazuh komut izleme yeteneği, belirli komutların çıktısını izlemenize ve çıktıyı günlük içeriği olarak ele almanıza olanak tanır. Komut izleme, disk alanı kullanımı, yük ortalaması, ağ dinleyicilerindeki bir değişiklik ve tüm önemli işlemlerin çalıştığından emin olmak için çalışan işlemler gibi çeşitli şeyleri izlemek için kullanılabilir.

Komut izleme, çeşitli anormallikleri ve tehditleri tespit etmek için kullanılabilir. Örneğin, komutun çıktısında bir değişiklik olup olmadığını izlemek için kullanabilirsiniz `netstat`; bu, yeni bir ağ dinleyicisinin eklendiğini veya kaldırıldığını gösterir. Ayrıca, komutun çıktısında belirli dizelerin varlığını izlemek için de kullanabilirsiniz `ps`; bu, kötü amaçlı bir işlemin çalıştığını gösterebilir.

Revision #2
Created 23 December 2024 18:29:11 by Ayşegül Sarıkaya
Updated 31 December 2024 17:59:31 by Ayşegül Sarıkaya