İzleme Sistemi Çağrıları

Linux uç noktalarındaki sistem çağrılarını izlemek, güvenlik denetimi amaçları için bilgi sağlar. Sistem çağrısı verilerini toplamak ve analiz etmek, güvenlik ekiplerinin şüpheli davranış kalıplarını belirlemesine ve olası güvenlik olaylarını zamanında araştırmasına yardımcı olur.

Linux Denetim sistemi, Linux uç noktalarındaki güvenlik ve güvenlik dışı olayları toplamak için güçlü bir araçtır. Ancak denetim günlükleri tarafından oluşturulan verilerin hacmi, sistem yöneticilerinin potansiyel güvenlik tehditlerini ve ihlallerini belirlemesini zorlaştırabilir.

Wazuh, Linux uç noktalarındaki sistem çağrılarını izlemek için Linux Denetim sistemini kullanır. Wazuh aracısı, sistem çağrısı olaylarını toplamak ve analiz için Wazuh sunucusuna göndermek üzere izlenen uç noktalara denetim kurallarını yükler ve yapılandırır. Bu denetim kuralları, güvenlik izlemeyle ilgili olayları yakalar. Wazuh, dosya erişimi, komut yürütme, ayrıcalık yükseltme, kötü amaçlı yazılım ve daha fazlası dahil olmak üzere birden fazla etkinliği algılamak için sistem çağrısı olaylarını kullanan kullanıma hazır algılama kuralları sağlar. Güvenlik ekipleri, bu kuralları belirli güvenlik gereksinimlerini veya uyumluluk standartlarını karşılayacak şekilde özelleştirebilir ve böylece olası güvenlik olaylarına ilişkin gerçek zamanlı içgörüler elde edebilir.

Wazuh, denetim olaylarının merkezi bir görünümünü sağlayarak sistem etkinliklerini izleme görevini basitleştirir ve kuruluşların düzenleyici gerekliliklere uymasına yardımcı olur. Genel olarak, Wazuh denetim yeteneği, Linux sistemleri için sağlam ve kapsamlı bir güvenlik izleme çözümü sunarak kuruluşların güvenlik duruşlarını iyileştirmelerine ve siber tehditlere karşı korunmalarına yardımcı olur.

Revision #2
Created 23 December 2024 18:28:12 by Ayşegül Sarıkaya
Updated 31 December 2024 18:00:05 by Ayşegül Sarıkaya