Wazuh Dashboard

Wazuh panosu, güvenlik olaylarını ve uyarı verilerini çıkarmak, analiz etmek ve görselleştirmek için esnek ve sezgisel bir web kullanıcı arayüzüdür. Ayrıca Wazuh platformunun yönetimi ve izlenmesi için de kullanılır. Ek olarak, rol tabanlı erişim kontrolü (RBAC) ve tek oturum açma (SSO) için özellikler sağlar.

Veri Görselleştirme ve Analizi

Web arayüzü, kullanıcıların Wazuh aracısı tarafından toplanan farklı veri türleri ve Wazuh sunucusu tarafından oluşturulan güvenlik uyarıları arasında gezinmesine yardımcı olur. Kullanıcılar ayrıca raporlar oluşturabilir ve özel görselleştirmeler ve panolar oluşturabilir.

Örneğin Wazuh, PCI DSS, GDPR, HIPAA ve NIST 800-53 gibi düzenleyici uyumluluk için kullanıma hazır panolar sağlar. Ayrıca MITRE ATT&CK çerçevesi ve ilgili uyarılar arasında gezinmek için bir arayüz sağlar.

• Uç nokta güvenliği • Güvenlik operasyonları	• Tehdit istihbaratı • Bulut güvenliği

Aracıların İzlenmesi ve Yapılandırılması

Wazuh panosu kullanıcıların aracı yapılandırmasını yönetmelerine ve durumlarını izlemelerine olanak tanır. Örneğin, izlenen her uç nokta için kullanıcılar hangi aracı modüllerinin etkinleştirileceğini, hangi günlük dosyalarının okunacağını, hangi dosyaların bütünlük değişiklikleri için izleneceğini veya hangi yapılandırma kontrollerinin gerçekleştirileceğini tanımlayabilir.

Ajanların izlenmesi

Platform Yönetimi

Wazuh dashboard (panosu), Wazuh dağıtımınızı yönetmeye adanmış bir kullanıcı arayüzü sağlar. Bu, farklı Wazuh bileşenlerinin durumunu, günlüklerini ve istatistiklerini izlemeyi içerir. Ayrıca Wazuh sunucusunu yapılandırmayı ve günlük analizi ve tehdit tespiti için özel kurallar ve kod çözücüler oluşturmayı içerir.

Platform yönetimi

Geliştirici Araçları

Wazuh panosu, günlük mesajlarını nasıl çözüldüğünü ve bir tehdit algılama kuralıyla eşleşip eşleşmediğini kontrol etmek için işleyebilen bir Kural Seti Test aracı içerir. Bu özellik, özel kod çözücüler ve kurallar oluşturulduğunda ve kullanıcı bunları test etmek istediğinde özellikle yararlıdır.



Wazuh panosu ayrıca kullanıcıların Wazuh API'siyle etkileşim kurması için bir API konsolu içerir. Bu, Wazuh dağıtımını yönetmek için kullanılabilir (örneğin, sunucu veya aracı yapılandırmalarını yönetmek, durumu ve günlük mesajlarını izlemek, aracıları eklemek veya kaldırmak vb.).



Revision #5
Created 6 December 2023 17:33:16 by LastGuard
Updated 11 December 2024 16:05:31 by Ayşegül Sarıkaya