Mevzuata Uygunluk Denetimi

Mevzuata uygunluk

Düzenleyici uyumluluk, hükümet organları, endüstri düzenleyicileri veya diğer yetkililer tarafından belirlenen yasaları, kuralları, düzenlemeleri ve standartları takip etmek anlamına gelir. Kuruluşların, iş operasyonlarının bütünlüğünü korumak ve hassas verileri korumak için düzenleyici uyumluluğa uymaları gerekir.

Düzenleyici gerekliliklere uymak, bir organizasyonun siber güvenlik çerçevesinin önemli bir bileşenini oluşturur. İlgili yasalar, kurallar ve ölçütlerle uyum sağlayarak, kuruluşlar bilgi kaynaklarını koruyabilir ve güvenlik ihlalleri olasılığını azaltabilir.

Wazuh, uyumluluğun uygulanması için çeşitli yetenekler sunar, bunlar arasında şunlar yer alır:

- Dosya Bütünlüğü İzleme (FIM).
- Güvenlik Yapılandırma Değerlendirmesi (SCA).
- Güvenlik açığı tespiti.
- Kötü amaçlı yazılım tespiti.
- Olay tepkisi.

Wazuh, PCI DSS, HIPAA, NIST 800-53, TSC ve GDPR çerçeveleri ve standartları için uyumluluk etiketlerine göre eşlenen kullanıma hazır kural kümeleri sağlar.

Mevzuata uygunluk modülleri

Wazuh, özel kurallar oluşturmanıza ve bunları ihtiyaçlarınıza uygun uyumluluk standartlarına etiketlemenize olanak tanır. Aşağıdaki bölüm, desteklenen standartlar için kullanım durumlarını ayrıntılı olarak açıklar.

PCI DSS

PCI DSS (Ödeme Kartı Endüstrisi Veri Güvenliği Standardı), kart verilerini işleyen, depolayan ve ileten işletmelerin uyması gereken güvenlik kriterlerini ana hatlarıyla belirtir. Bu standart, kart sahibi verilerini çevreleyen güvenlik önlemlerini sıkılaştırmak ve ödeme kartı endüstrisindeki dolandırıcılığı azaltmak için tasarlanmıştır.

Ödeme kartı endüstrileri, PCI DSS uyumluluğunu güçlendirmek için Wazuh yeteneklerinden yararlanabilir. Kullanıcılar, bu yetenekleri, standart tarafından belirtildiği gibi belirli iş ihtiyaçlarıyla uyumlu hale getirmek için özelleştirebilir. Örneğin, maskelenmemiş bir Birincil Hesap Numarasının (PAN) varlığını algılayan gümrük kuralları oluşturarak bir PAN taraması yapmak için Wazuh'u kullanabilirsiniz .

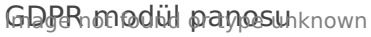


Maskelenmemiş Birincil Hesap Numarası (PAN) uyarısı

Wazuh'un kuruluşların PCI DSS standardını karşılamasına nasıl yardımcı olduğu hakkında daha fazla bilgi edinebilirsiniz .

GDPR

Avrupa Birliği tarafından geliştirilen Genel Veri Koruma Yönetmeliği (GDPR), kıta genelinde veri gizliliği yasalarını uyumlu hale getirmeyi amaçlamaktadır. Avrupa Birliği vatandaşlarının verilerinin korunması başlıca önceliğidir. GDPR çerçevesi, kullanıcı veri gizliliğini artırmayı ve Avrupa Birliği'nin ve AB vatandaşlarının verilerini işleyen kuruluşların veri gizliliğini nasıl ele aldığını değiştirmeyi amaçlamaktadır.



GDPR modül panosu

Wazuh, farklı siber saldırı türlerini, yanlış yapılandırılmış sistemleri, güvenlik açıklarını ve politika ihlallerini tanımlamak için varsayılan kurallar ve kod çözücülerle birlikte gelir. Bu olaylar ilgili GDPR gerekliliklerine etiketlenir. Wazuh'un kuruluşların GDPR düzenleme uyumluluğunu karşılamasına nasıl yardımcı olduğu hakkında daha fazla bilgi bulabilirsiniz .

HIPAA

Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası, sağlık kuruluşlarının ve organizasyonlarının hassas hasta sağlık bilgilerinin yetkisiz ifşasını önlemesini sağlayan yasal bir çerçevedir. Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası (HIPAA), sağlık hizmetlerinin verimliliğini artırmak için sağlık bilgilerinin işlenmesine ilişkin yönergeler ve prosedürler belirler. Elektronik sağlık hizmetleri işlemleri için yönergeler ve güvenlik ve ayırt edici sağlık kimliği standartları içerir.

HIPAA çerçevesi, bu bilgilerin gizliliği ve güvenliği üzerinde etkisi olan teknolojik gelişmeler nedeniyle sağlık bilgileri için federal gizlilik korumaları gerektirmektedir.

Kuruluşlar, Wazuh FIM modülünü kullanarak PII (kişisel olarak tanımlanabilir bilgiler) ve diğer gizli belgelere erişimi ve bunlarda yapılan değişiklikleri izleyebilir .

Wazuh'un kuruluşların HIPAA çerçevesini karşılamalarına nasıl yardımcı olduğu hakkında daha fazla bilgi bulabilirsiniz .

Aşağıdaki görüntü, izlenen bir uç noktada bir dosyanın oluşturulmasını ve silinmesini göstermektedir.



Oluşturulan ve silinen dosyanın FIM uyarısı

NIST 800-53

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) 800-53, Federal Bilgi Sistemleri ve Kuruluşları için Güvenlik ve Gizlilik Kontrolleri olarak bilinir. Daha büyük NIST Özel Yayını 800 serisinin önemli bir bileşenidir.

NIST 800-53, federal kuruluşlar ve ajanslar için bilgi güvenliği ve gizliliğini yönetmeye yönelik öneriler sunar. Kuruluşların hassas verileri korurken bilgi sistemlerini ve verilerini çeşitli tehditlerden korumasına yardımcı olur.



NIST 800-53 modül gösterge paneli

Güvenlik açığı tespit modülü sonuçlarını, izlenen uç noktadaki güvenlik açığı uygulamalarını ve paketlerini içeren Wazuh panosunda görüntüleyebilirsiniz . Wazuh'un kuruluşların NIST 800-53 standardını karşılamalarına nasıl yardımcı olduğu hakkında daha fazla bilgi bulabilirsiniz .

Güvenlik Açığı Tespiti modülü envanteri

TŞK

Güven Hizmetleri Kriterleri, AICPA'nın Güvence Hizmetleri Yürütme Komitesi (ASEC) tarafından geliştirilmiştir. TSC'nin güvenlik, kullanılabilirlik, işlem bütünlüğü, gizlilik ve mahremiyet olmak üzere beş güven hizmeti alanı vardır. Kuruluşlar, müşteri verilerini yetkisiz erişim, kullanım, ifşa, değişiklik veya imhadan korumak için TSC'yi uygular.

Wazuh, kuruluşlara bilgi güvenliği politikalarının etkinliğini değerlendirmeleri ve raporlamaları için standart bir yol sağlayan TSC Ortak Kriterleri için kullanıma hazır etiketler sağlar. Wazuh'un

kuruluşların TSC uyumluluğunu nasıl karşılamasına yardımcı olduğu hakkında daha fazla bilgi bulabilirsiniz .

Aşağıdaki resim, Wazuh'un kuruluşların CC7.2 - Olaylara işaret eden tüm düzensiz faaliyetlerin sürekli izlenmesini gerektiren - karşılamalarına yardımcı olduğu bazı Ortak kriterleri göstermektedir .

TSC ortak kriterlere uyum

Image not found or type unknown

Revision #4
Created 6 December 2023 18:03:35 by LastGuard
Updated 11 December 2024 22:21:43 by Ayşegül Sarıkaya