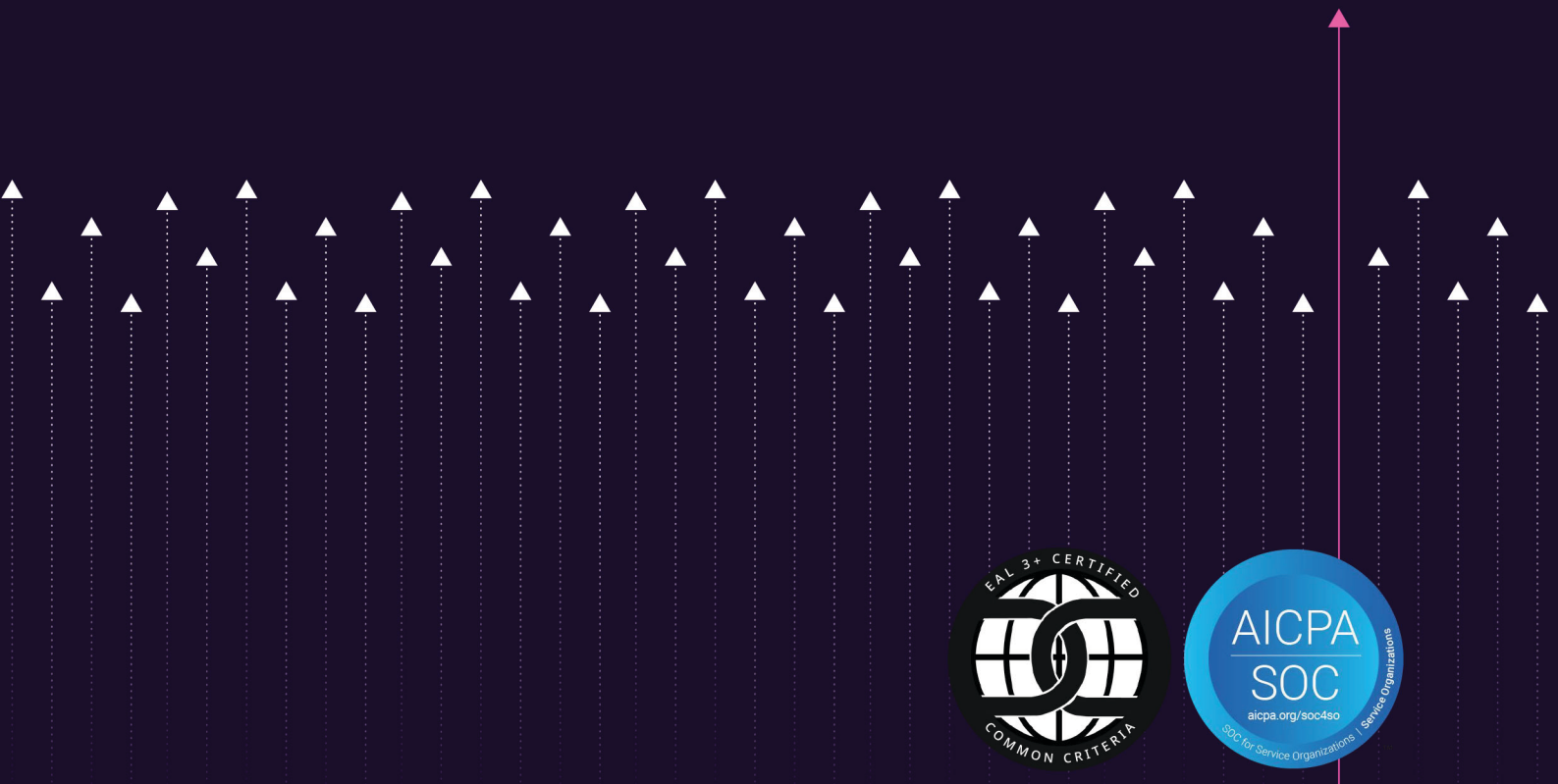
guardsix SIEM



OTD BİLİŞİM

GLOBAL VAD

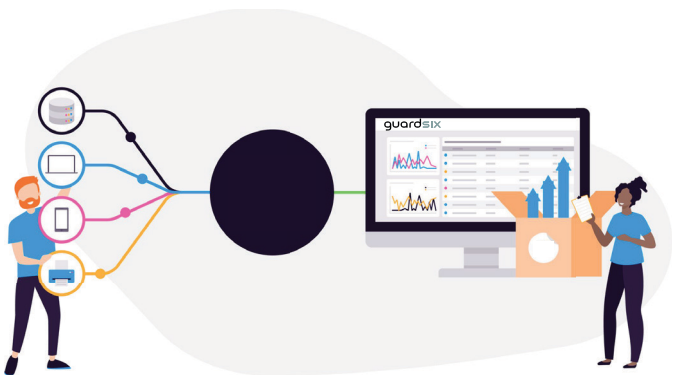
KULLANIM SENARYOSU KILAVUZU: GUARDSIX SIEM

Guardsix SIEM'in en son sürümü; güvenlik operasyonlarını, Ortalama Yanıt Süresini (MTTR), tehdit avcılığını ve log toplamayı optimize etmek üzere tasarlanmış yeni özelliklerle birlikte sunulmaktadır. Genel olarak Guardsix, güvenlik duruşunuzun kesintisiz bir şekilde iyileştirilmesini sağlamayı amaçlamaktadır. Bu kullanım senaryosu kılavuzu, iki temel özellik hakkında bilgi sunacaktır: Default Syslog Accept ve log kaynaklarının izlenmesine yönelik durum göstergeleri.

Default Syslog: Kullanıma hazır Syslog log alımı desteğiyle basitleştirilmiş SIEM kurulumu

Hızlı ve verimli log alımı yalnızca teknik bir ayrıntı değil; güçlü bir güvenlik duruşunun sürdürülmesine yardımcı olan etkili ve sorunsuz güvenlik operasyonları için temel bir gereksinimdir. Log kaynaklarınızı log alımı için nasıl yapılandırdığınız, SIEM kurulum sürecinin hızını belirler.

Guardsix'in en son sürümü, manuel yapılandırmanın karmaşıklığını ortadan kaldırır ve kurulumdan hemen sonra logların toplanmasını sağlar. Syslog mesajlarının varsayılan olarak kabul edilmesine olanak tanıyan Guardsix; kurulum süresini azaltır, güvenlik iş akışlarını kolaylaştırır ve olay müdahale süreçlerini iyileştirir. Syslog log alımı için kullanıma hazır olarak sunulan bu destek sayesinde Guardsix, sorunsuz devreye alma deneyimi ve ölçeklenebilirlik sağlar. Default Syslog log alımı, gerektiğinde sistem ayarlarından devre dışı bırakılabilir.



Yeni kurulumlar için anında log toplama

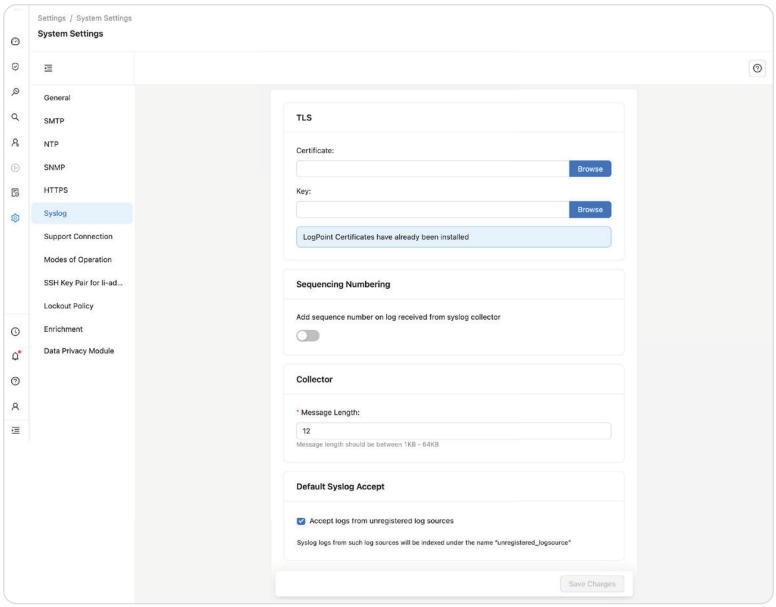
Default Syslog, güvenlik ekiplerinin ilk günden itibaren logları sisteme almasını sağlayarak ilk kurulum aşamasında kritik logların kaybolmasını önler. Manuel yapılandırmaların ortadan kaldırılması sayesinde kuruluşlar, güvenlikle ilgili hiçbir verinin gözden kaçmamasını sağlar.

MSSP'ler için optimize edilmiş log toplama

Yönetilen Güvenlik Hizmeti Sağlayıcıları (MSSP'ler), tüm müşteri loglarının veri kaybı olmadan toplandığından emin olmalıdır. Anında log alımı sayesinde Default Syslog, devreye alma sürecini kolaylaştırır ve güvenlik verilerinin kesintisiz kullanılabilirliğini sağlar.

Uzun vadeli veri bütünlüğü için özelleştirilebilir

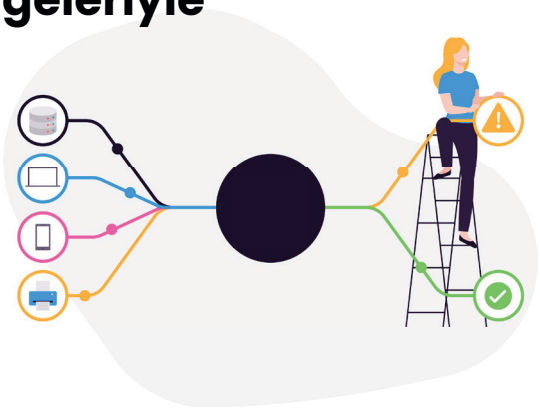
Default Syslog kolay bir başlangıç sağlarken ekipler, yapılandırılmış log alımını sağlamak için daha sonra kaynakları ve normalizer'ları yapılandırabilir. Bu yapılandırmalar olmadan bazı loglar tam olarak ayrıştırılamayabilir ve bu durum analitik içgörüleri sınırlayabilir.



Veri boşlukları olmadan ölçeklendirme

İşletmeler ölçeklendikçe yeni Guardsix instance'larının eklenmesi, yapılandırmaların doğru şekilde yapılmaması durumunda geçici log kaybına yol açabilir. Default Syslog, logları otomatik olarak kabul ederek bunu önler ve veri toplama sürekliliğini sağlar.

Log Kaynağı aktivitesi: Durum göstergeleriyle proaktif Log Kaynağı izleme



Kesintisiz log toplama, SIEM'in etkinliğini sağlayan temel unsurdur ve güvenlik ekiplerinin görünürlüğü korumasına ve tehditlere etkili bir şekilde yanıt vermesine olanak tanır. Ancak aktif olmayan log kaynaklarının zamanında tespit edilmesi, geleneksel olarak manuel çaba gerektirmiştir. Guardsix'in en son sürümü, proaktif sorun çözümünü sağlamak amacıyla son alınan log durumunun yanında otomatik izleme ve renk kodlu göstergeler sunarak bu süreci kolaylaştırır.

Kesintisiz log toplama, SIEM'in etkinliğini sağlayan temel unsurdur ve güvenlik ekiplerinin görünürlüğü korumasına ve tehditlere etkili bir şekilde yanıt vermesine olanak tanır. Ancak aktif olmayan log kaynaklarının zamanında tespit edilmesi, geleneksel olarak manuel çaba gerektirmiştir. Guardsix'in en son sürümü, proaktif sorun çözümünü sağlamak amacıyla son alınan log durumunun yanında otomatik izleme ve renk kodlu göstergeler sunarak bu süreci kolaylaştırır. Guardsix SIEM, manuel sorgular çalıştırmaya gerek kalmadan log kaynağı aktiviteleri üzerinde gerçek zamanlı görünürlük sağlar. Önceden tanımlanmış zaman eşiklerine dayalı görsel durum sistemi sayesinde güvenlik ekipleri, aksi takdirde fark edilmeyebilecek log kaynağı inaktivitesini tespit edebilir ve giderebilir. Bu özellik, log kaynaklarının izlenmesine yönelik daha sezgisel ve otomatik bir yaklaşım sunarak güvenlik operasyonlarını geliştirir, yanıt sürelerini iyileştirir ve kritik log kaybını önler. Yapılandırılabilir renk kodlu göstergelere ek olarak, kesintisiz log toplamayı sağlamak amacıyla uyarılar ve bildirimler alınabilir; böylece güvenlik duruşu ve operasyonel verimlilik iyileştirilir.

Aktif olmayan log kaynaklarını anında tespit edin

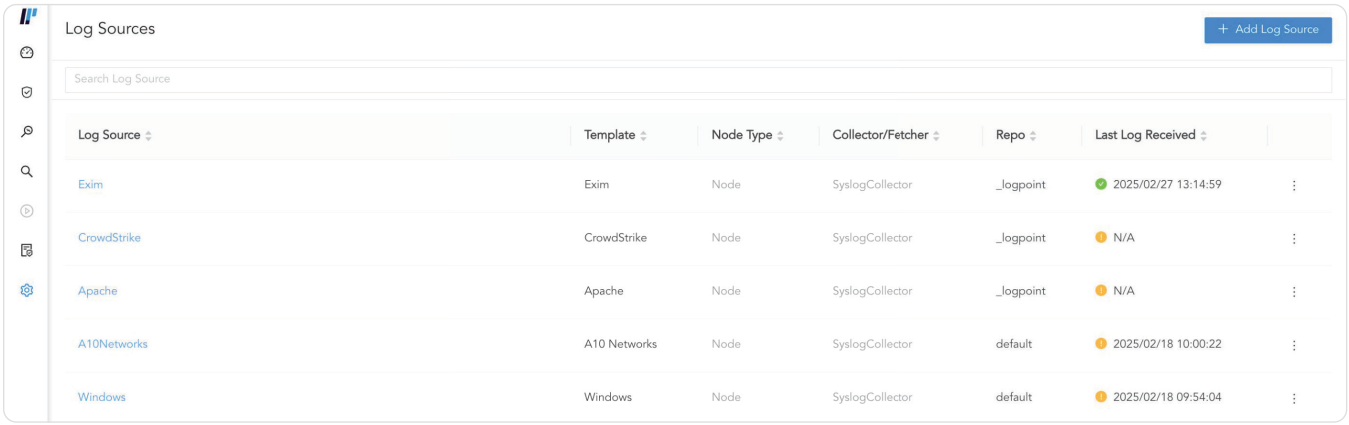
Guardsix'in log kaynağı izleme özelliğindeki geliştirmeler, güvenlik ekiplerinin log kaynağı hatalarını anında tespit etmesine ve gidermesine olanak tanır. Gerçek zamanlı izleme ve otomatik bildirimler, güvenlik analizindeki kör noktaların önlenmesine yardımcı olarak tespit edilemeyen inaktivite nedeniyle hiçbir logun gözden kaçmamasını sağlar.

Birden fazla kanal üzerinden kesintisiz uyarı

Guardsix; e-posta, platform içerisindeki Guardsix bildirimleri veya SNMP izleme entegrasyonu aracılığıyla uyarılar yapılandırmanıza olanak tanıyarak ekibinizin kritik log kaynağı hatalarını hiçbir zaman gözden kaçırmamasını sağlar. Böylece mevcut izleme yapılarıyla sorunsuz bir uyarı mekanizması sağlanır.

Büyük ölçekli kurulumlara sahip kuruluşlar için ideal:

Büyük ölçekli log kaynaklarını yöneten kuruluşlar, log yönetimi operasyonlarını kolaylaştırmak için log kaynağı izleme özelliğinin SNMP entegrasyonundan yararlanabilir. İnaktivite tespitinin otomatikleştirilmesi ve SNMP uyarılarının gönderilmesi sayesinde log kaynakları daha geniş BT altyapısıyla birlikte izlenebilir; böylece proaktif sorun tespiti sağlanır, operasyonel yük azaltılır ve büyük ölçekte kesintisiz log toplama sürdürülebilir.



Daha kolay izleme için renk kodlu göstergeler

Renk kodlu durum sistemi sayesinde kullanıcılar, log kaynağı aktivitesini görsel olarak kolayca belirleyebilir:

- **Yeşil:** Aktif log kaynağı
- **Sarı:** Aktif olmayan log kaynağı

Bu hızlı görsel referans, sorun giderme süresini azaltır ve sorunların daha hızlı giderilmesini sağlar.

Operasyonel verimlilik için özelleştirilebilir:

Log kaynağı izleme özelliği, kullanıcıların kaynak türüne bağlı olarak kaynak inaktivitesi için eşik değerleri yapılandırmasına olanak tanır. Güvenlik ekipleri, bir kaynak düzensiz olarak işaretlenmeden önce inaktivite sürelerini tanımlayabilir; böylece gereksiz uyarılar azaltılır ve aksiyon alınabilir içgörüler elde edilmesi sağlanır.

guardsix

OTD BİLİŞİM
GLOBAL VAD