KLOG SERVER

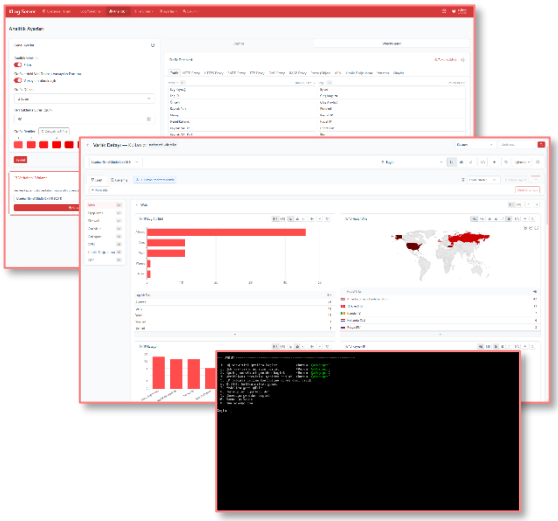
LOG İMZALAMA, ARŞİVLEME ve ANALİZ ÇÖZÜMÜ

KLog Server

KLog Server, 5651 sayılı Kanun'a uygun zaman damgası hizmeti sunan gelişmiş bir Syslog sunucusudur. Syslog toplamanın yanı sıra, paylaşımlı klasörlerden, AWS S3 ve Azure Files bulut depolama platformlarından log toplama ve dijital olarak imzalama yeteneklerine de sahiptir. Linux tabanlı olarak geliştirilen KLog Server, VMware, Microsoft Hyper-V ve Proxmox sanallaştırma platformlarıyla uyumlu, kullanıma hazır sanal makine olarak sunulmaktadır.

KLog Server, üretici bağımsız olarak, standart Syslog protokolü ile log üreten tüm cihazlarla (güvenlik duvarları, sunucular, vb.) entegre çalışır. Gün boyunca aldığı logları, her gün sonunda Kamu SM (Kamu Sertifikasyon Merkezi) onaylı bir sertifika ile elektronik olarak imzalar ve log dosyalarını imza dosyaları ile birlikte güvenle depolar.

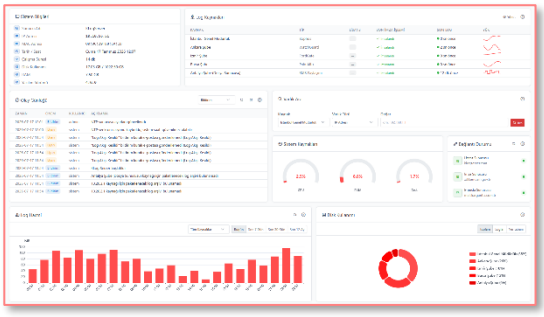
Özellikler

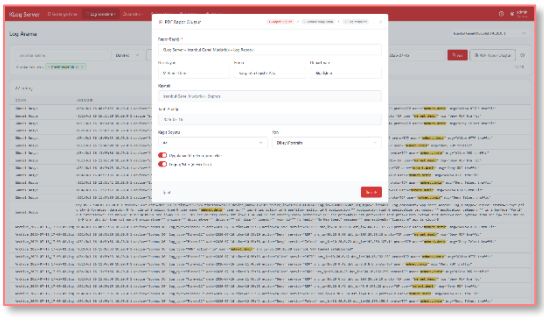


- Kamu SM onaylı SHA-512 karma algoritması ile güvenli log imzalama desteği
- Web tabanlı yönetim paneli ve konsol arayüzü
- Hızlı kurulum ve kolay yapılandırma
- Log üreten cihazların otomatik keşfi ve log toplama
- Paylaşımlı klasörlerden (SMB) log toplama ve imzalama desteği
- AWS S3 ve Azure Files platformlarından log toplama ve imzalama desteği
- Anlık log izleme ve gelişmiş log arama
- Toplanan loglardan 700'den fazla kapsamlı analiz grafiği oluşturma
- Log Arama ve Analitik sayfalarında sihirbaz destekli PDF ve CSV raporlama
- Belirlenen kurallara uyan loglar için otomatik uyarı ve e-posta bildirimleri
- Gösterge Paneli üzerinden imzalama durumunun anlık takibi
- Web arayüzü üzerinden imzalanmış log ve imza dosyalarının indirilmesi
- İmzalanmış logların FTP, SCP sunucularına veya paylaşımlı klasörlere günlük ya da toplu olarak otomatik aktarımı
- Bayi ve son kullanıcı yapıları için çoklu yönetici desteği

Gösterge Paneli

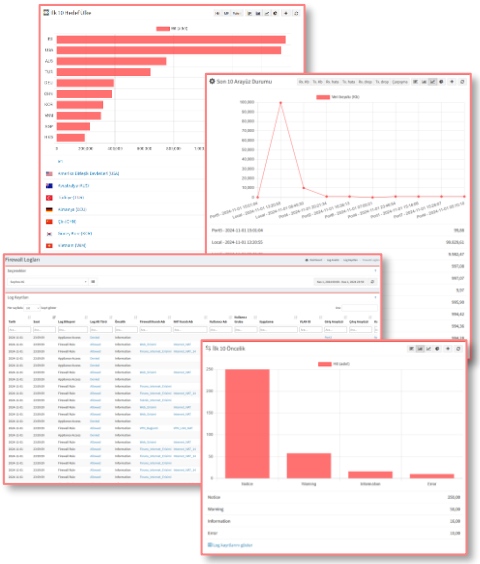
Gösterge Paneli, sistem durumu ile log toplama ve imzalama süreçlerine ilişkin kritik bilgileri tek ekranda sunar. Bu ekranda işlemci, bellek ve disk kullanımına ait sistem bilgileri görüntülenir. Ayrıca, her bir log kaynağı için lisans durumu, son imzalama işleminin durumu ve alınan son log kaydının zamanı izlenebilir. Gösterge Paneli, bunun yanı sıra her log kaynağına ait canlı log boyutunu grafiksel olarak göstererek sistemin anlık durumunun kolayca takip edilmesini sağlar.





Log İçeriği İzleme ve Loglarda Arama

Alınan loglar, Canlı Log ekranı üzerinden anlık olarak izlenebilir. Log arama özelliği sayesinde, imzalama bekleyen veya imzalanmış loglar; log kaynağı, tarih ve anahtar kelime kriterlerine göre hızlı ve kolay bir şekilde sorgulanabilir. Elde edilen sonuçlar web arayüzü üzerinden görüntülenebilir veya sihirbaz yönlendirmeli ayrıntılı PDF raporları olarak oluşturulabilir.

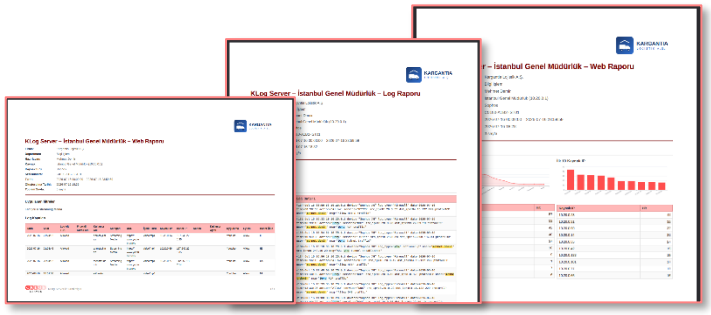


Log Analizi ve Raporlama

Log analizi özelliği, Sophos ve WatchGuard güvenlik duvarlarından toplanan log verilerini gerçek zamanlı olarak görselleştirerek anlamlı içgörüler sunar; oluşum sayısı, veri hacmi ve paket sayısı gibi metrikleri grafiklerle gösterir. Yöneticiler, çubuk, çizgi, pasta ve harita grafik türleri arasında kolayca geçiş yapabilir. KLog Server; IP adresi, MAC adresi, kullanıcı, dosya, alan adı, URL ve kural/ilke gibi varlıkları otomatik olarak tanır, tek tıkla bu varlıklara ait log aktivitelerini bir arada sunar ve web, uygulama, güvenlik duvarı, VPN ve kimlik doğrulama gibi farklı log türlerine bütünsel bir bakış sağlar.

Her grafik, logların tablo formatında incelenmesine olanak tanır. Tablolar; anahtar kelime ile arama, zaman aralığı, basit ve gelişmiş filtreleme özellikleri sayesinde geniş log verileri arasında kolay gezinme sağlar. Daha anlaşılır bir analiz için KLog Server, IP adreslerini ülke bayrakları ile ve MAC adreslerini üretici ikonları ile eşleştirir.

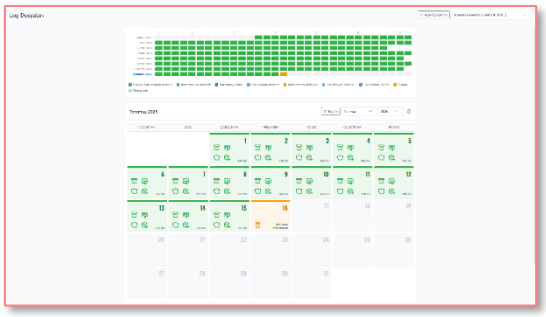
Log Arama ve Analitik sayfalarında sihirbaz yönlendirmeli ayrıntılı PDF rapor oluşturma özelliği sunulur. Rapor hazırlama sihirbazı sayesinde kullanıcılar, raporda yer alacak grafik ve kolonları kolayca seçebilir, belirlenen anahtar kelimelerin vurgulanması için özel kurallar oluşturabilir. Ayrıca, imzalanmış dosyalara ait bilgilerin de rapora dahil edilmesine olanak sağlanır.



Log Dosyaları Dışa Aktarma

Günlük log dosyaları, imzalama işlemi tamamlandıktan sonra veya geriye dönük olarak toplu şekilde, imza dosyalarıyla birlikte otomatik olarak dışa aktarılabilir. Desteklenen harici depolama alanları arasında FTP sunucusu, SCP sunucusu ve paylaşımlı klasörler bulunmaktadır. Dışa aktarılan dosyalar, disk alanı yönetimini kolaylaştırmak amacıyla isteğe bağlı olarak sistemden silinebilir.

Log dosyalarının dışa aktarımına ek olarak, dosyalar web arayüzünden indirilebilir veya disk alanı yönetimini kolaylaştırmak amacıyla sistemden silinebilir.

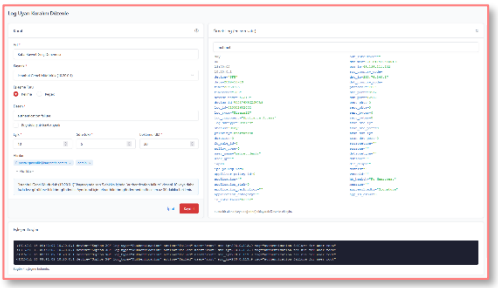


Çoklu Yönetici Yapısı

KLog Server, yönetici veya bayi/müşteri yapısını destekleyerek çoklu kullanıcı yönetimi imkanı sunar. Birden fazla kullanıcı hesabı tanımlanabilir ve log kaynakları belirli kullanıcılara atanabilir. Kullanıcılar yalnızca kendilerine yetkilendirilen log kaynaklarına ve ilgili menülere erişebilirken, Admin kullanıcı tüm kaynaklara tam erişim sağlayabilir. Tüm kullanıcı işlemleri sistem tarafından kayıt altına alınarak denetlenebilir. Bu yapı, çoklu lokasyon/şube ve merkezi log toplama senaryolarında etkin hiyerarşik yönetim imkanı sunar.

Log Uyarıları ve Bildirim

KLog Server, belirlenen düz metin veya Regex koşullarına uyan logları otomatik olarak algılayarak anlık uyarı oluşturur ve e-posta ile bildirim gönderir. Bunun yanı sıra, log alınamaması, imzalama işleminin başarısız olması, disk alanının azalması gibi sistem olaylarında da bildirim sağlar. Bildirimler; yöneticiye, kaynak sahibine veya özel e-posta adreslerine gönderilebilir.



Kamu SM Onaylı Zaman Damgası

KLog Server tarafından imzalanan logların Kamu SM onaylı olduğunu TÜBİTAK BİLGEM tarafından geliştirilen Kamu SM Zaman Damgası uygulaması ile doğrulayabilir ve her log dosyası için sertifika bilgilerini içeren beraat belgesini indirebilirsiniz.

Daha fazla bilgi: www.klogserver.com