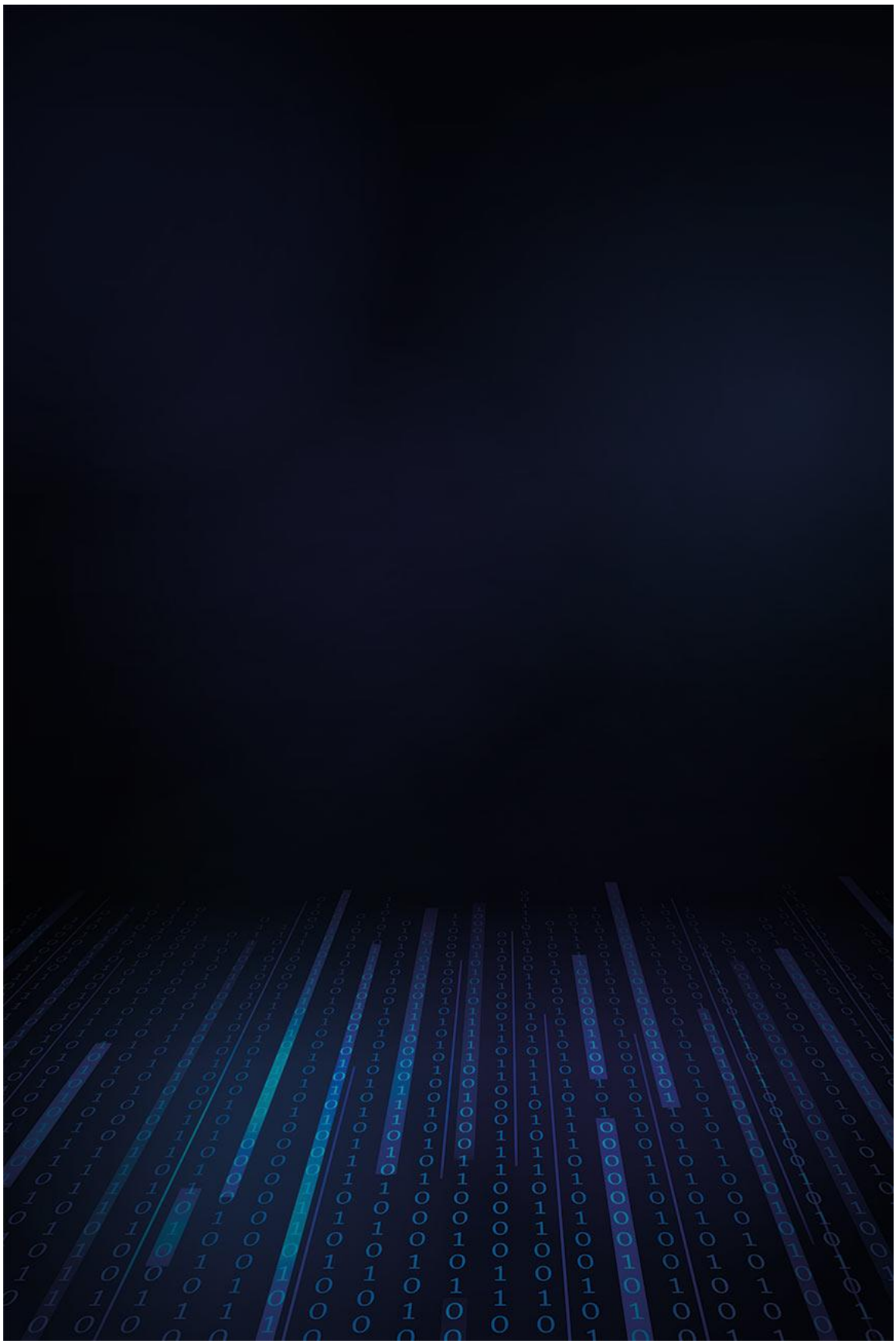


.oriana

İçindekiler

.oriana

.oriana

OrianaLOG Hakkında

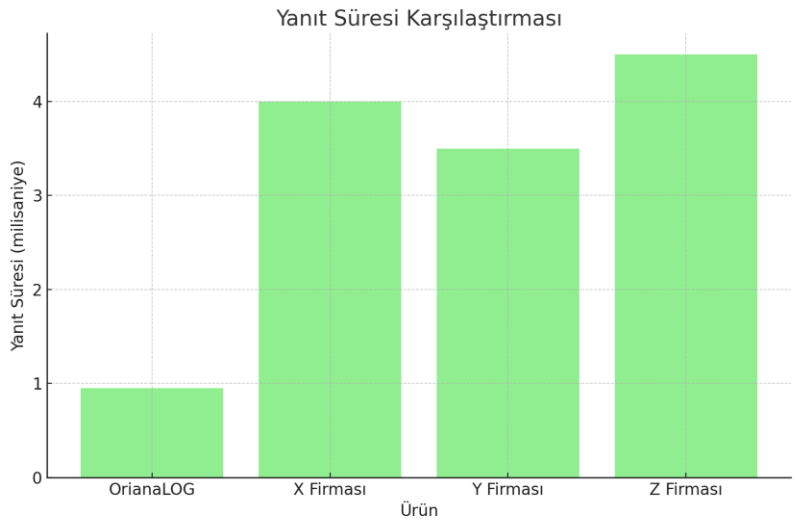
Neden .OrianaLOG?

.OrianaLOG, merkezi log yönetimi, gerçek zamanlı izleme ve analiz, olay korelasyonu, özelleştirilebilir dashboardlar, raporlama ve uyarı sistemleri gibi kapsamlı özellikler sunar. Güvenlik olaylarını tespit etme, hata ayıklama ve performans izleme gibi görevlerde etkilidir. .OrianaLOG, kullanıcı dostu arayüzü ve yüksek performansıyla log yönetimini kolaylaştırır ve güvenlik süreçlerinizi optimize eder.

Aşağıdaki grafikler, .OrianaLOG'un rakiplerine göre avantajlarını göstermektedir.

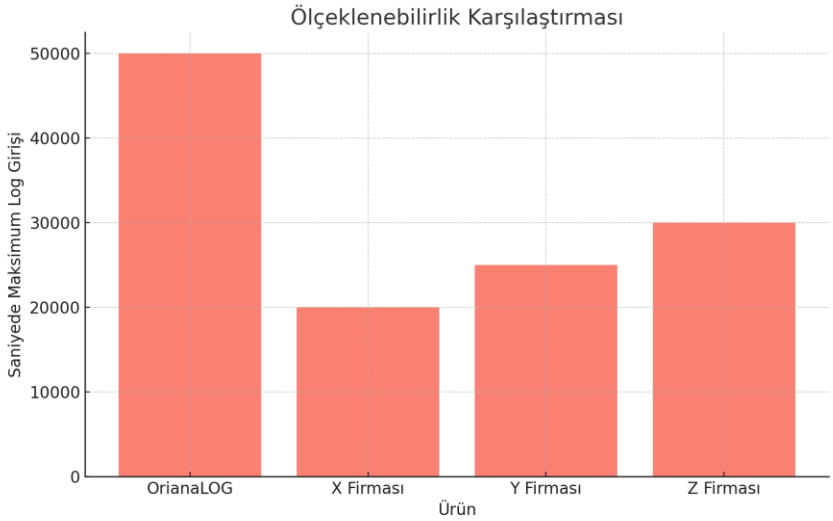
Yanıt Süresi Karşılaştırması

OrianaLOG'un gerçek zamanlı izleme ve analiz kapasitesi, rakiplerine göre daha hızlıdır. Aşağıdaki grafikte de görüldüğü gibi, .OrianaLOG'un yanıt süresi rakip ürünlerden daha kısadır (ortalama 0.95 ms).



Ölçeklenebilirlik Karşılaştırması

OrianaLOG'un yüksek performans ve ölçeklenebilirliği, büyük veri setlerini etkili bir şekilde işlemesine olanak tanır. Aşağıdaki grafikte, .OrianaLOG'un saniyede işleyebildiği maksimum log girişi sayısı rakiplerine göre oldukça yüksektir. .OrianaLOG, saniyede tek sunucuda 50,000 log girişi işleyebilir; daha fazla log girişini ise cluster yapısı ile toplayabilir.



.OrianaLOG'un öne çıkan farklılıkları ve özellikleri nelerdir?

Merkezi Log Yönetimi: Farklı kaynaklardan gelen log verilerini merkezi bir noktada toplar ve yönetir.
Gerçek Zamanlı İzleme ve Analiz: Log verilerini anında analiz ederek olası güvenlik tehditlerini hızlıca tespit eder. .OrianaLOG'un yanıt süresi ortalama 0.95 ms'dir ve bu süre, X Firması gibi rakip ürünlerde ortalama 4 ms'dir.
Olay Korelasyonu: Log verilerini analiz ederek olası güvenlik olaylarını ilişkilendirir ve tespit eder.
Özelleştirilebilir Dashboardlar: Kullanıcıların ihtiyaçlarına göre özelleştirilebilen dashboardlar sunar.
Raporlama ve Uyarı Sistemleri: Özelleştirilebilir raporlar ve uyarılar ile sistem yöneticilerine ve güvenlik ekiplerine önemli bilgiler sunar.
Uyumluluk Yönetimi: Belirli uyumluluk standartlarını karşılamak için gerekli araçları sağlar.
Yüksek Performans ve Ölçeklenebilirlik: Büyük ölçekli log verilerini işleyebilecek kapasiteye sahiptir. .OrianaLOG, saniyede tek sunucuda 50,000 log girişini işleyebilir; daha fazla log girişini ise cluster yapısı ile toplayabilir.
Kullanıcı Dostu Arayüz: Kullanımı kolay ve anlaşılır bir arayüz sunar.

.OrianaLOG'un veri toplama yetenekleri nelerdir?

OrianaLOG, sunucular, depolama üniteleri, parmak izi okuma sistemleri, anti-virüs yazılımları, veri kaybını önleme (DLP) çözümleri ve güvenlik duvarları (firewall) gibi çeşitli

cihazlardan gelen verileri toplar ve merkezi bir yönetim altında analiz eder. Ayrıca IoT cihazları, ağ anahtarları ve yönlendiriciler gibi daha geniş bir cihaz yelpazesinden de veri toplayabilir.

.OrianaLOG'un rekabet avantajları nelerdir?

.OrianaLOG, düşük maliyet ve yüksek performans, düzenli bakım kontrolleri, hızlı güncellemeler ve etkin müşteri desteği gibi rekabet avantajlarına sahiptir. .OrianaLOG'un maliyetleri, verimli kaynak kullanımı ve optimize edilmiş altyapısı sayesinde rakiplerine göre daha düşüktür. Ayrıca, veri etiketleme, veri tekilleştirme ve Docker desteği gibi benzersiz özellikleriyle öne çıkar.

.OrianaLOG'un kullanıcı arayüzü nasıldır?

OrianaLOG, kullanıcı dostu ve anlaşılır bir arayüze sahiptir. Bu sayede log yönetimi ve analiz işlemleri daha az karmaşık hale gelir ve kullanıcıların sistemle etkileşimini kolaylaştırır.

.OrianaLOG SIEM Olarak Kullanılabilir mi?

.OrianaLOG geleneksel SIEM'ler gibi korelasyon motoruna sahiptir. Fakat, .OrianaLOG tek kurallı korelasyonlar oluşturabildiği için tam anlamıyla bir SIEM değildir.
.OrianaLOG 'one shot correlation' olarak bilinen benzersiz bir korelasyon özelliği ile donatılmıştır. Bu özellik yazılımın loglar arasında tek atımlık korelasyon gerçekleştirmesini sağlar ve log verilerinde belirli kalıpların veya olayların tespit edilmesine imkan tanır. Bu işlevsellik anormallikleri, güvenlik olaylarını veya diğer kritik olayları gerçek zamanlı olarak tespit etmek isteyen kuruluşlar için özellikle faydalıdır. .OrianaLOG bu özellikleri basitleştirerek maliyeti düşük tutar ve sadece ihtiyaç duyulan temel korelasyonları sağlar. Örnek olarak, izinsiz dosya paylaşımı, şüpheli ağ trafiği, ve yetkisiz yazılım yükleme denemeleri gibi olayları tek atımlık korelasyonlarla tespit edebilir.

.OrianaLOG Dil Desteği Var Mı?

.OrianaLOG **Türkçe**, İ**ngilizce**, **Almanca** ve **Fransızca** dil desteği sunmaktadır.

.OrianaLOG Hangi Sistemlerde Çalışıyor?

.OrianaLOG Multi Platform olarak geliştirilmiştir. Bu sayede tüm işletim sistemleri için dağıtılabilmektedir. Ayrıca .OrianaLOG docker üzerine kurulabildiğinden Docker bulunan tüm ortamlarda rahatlıkla kurularak kullanılabilir.

.OrianaLOG için Sistem Kaynak İhtiyaçları Nedir?

.OrianaLOG için sistem kaynak ihtiyaçları değişkendir. EPS (Event per Second - Saniye Başı Olay) değeri üzerinden yapılan testler sonucunda en doğru kaynak ihtiyaçları belirlenebilmektedir.

.oriana

.OrianaLOG'da Fiyatlandırma Nasıl Belirleniyor?

.OrianaLOG'da fiyatlandırma EPS (Event per Second - Saniye Başı Olay) değeri üzerinden hesaplanmaktadır. Ayrıca kaynak sayısına göre de fiyatlandırma seçenekleri mevcuttur.

.OrianaLOG Kurulumu Nasıl Yapılıyor?

.OrianaLOG docker üzerinde çalışabildiği için kurulum scripti ile birlikte kolayca kurulabilmektedir.

.OrianaLOG MSSP Özelliklerini Destekliyor Mu?

.OrianaLOG MSSP özelliklerine sahiptir. Gelişmiş kullanıcı rol yönetimi sistemi sayesinde arayüzde bulunan sayfa, buton ve aksiyonlara (Ekle, Sil, Güncelle, Görüntüle) ayrı ayrı yetkilendirmeler yapılabilmektedir. .OrianaLOG ile bir kullanıcının yalnızca görme yetkisine sahip olduğu cihazları görüntülemesi, sadece o cihazlar üzerinde işlemler yapabilmesi gibi gelişmiş yetki ve rol yönetimleri mümkündür.

.OrianaLOG Hangi Açık Kaynak Servisleri Kullanıyor?

.OrianaLOG işlevselliğini artırabilmek için aşağıdaki açık kaynak servisleri kullanmaktadır:
• **Redis**: Açık kaynaklı bir veri yapısı sunucusudur. Redis, BSD lisansı altında dağıtılmaktadır.
• **RabbitMQ**: Açık kaynaklı bir mesaj kuyruklama sistemidir. RabbitMQ, Mozilla Public License 2.0 (MPL) altında lisanslanmıştır.

.OrianaLOG Ajanı ile Hangi Loglar Toplanabilmektedir?

.OrianaLOG Ajanı ile aşağıdaki loglar toplanabilmektedir;

1. **Sistem Logları Windows Event Logları**: Windows Event Log (EVTX) dosyalarını ve eski Windows Event Log (EVT) formatlarını okuyabilir. Linux/Unix Sistem Logları: Linux ve Unix sistemlerindeki syslog, rsyslog, ve syslog-ng gibi logları toplayabilir. Sistem Dosya Logları: /var/log gibi Linux/Unix sistemlerinde bulunan sistem dosya loglarını okuyabilir.
2. **Uygulama Logları Text Log Dosyaları**: Uygulamaların ürettiği düz metin log dosyalarını okuyabilir. JSON ve XML Logları: JSON ve XML formatındaki log dosyalarını destekler ve bu formatlardan veri toplayabilir. CSV Log Dosyaları: CSV (Comma Separated Values) formatındaki logları işleyebilir.
3. **Ağ Logları Syslog**: RFC 3164 ve RFC 5424 uyumlu syslog mesajlarını alabilir ve işleyebilir. HTTP/S: HTTP ve HTTPS üzerinden gelen logları alabilir. SNMP Traps: SNMP protokolü üzerinden gelen trap mesajlarını toplayabilir.
4. **Veritabanı Logları SQL Logları**: SQL sorguları çalıştırarak veritabanlarından log verilerini çekebilir. ODBC ve JDBC: ODBC veya JDBC üzerinden veritabanlarına bağlanarak log verilerini alabilir.
5. **Özel ve Üçüncü Taraf Logları Apache ve Nginx Logları**: Web sunucusu loglarını toplayabilir. IIS Logları: Microsoft IIS web sunucusu loglarını işleyebilir. Firewall ve

IDS/IPS Logları: Ağ güvenlik cihazlarından gelen logları alabilir. Custom Log Formatları: Kullanıcının tanımlayabileceği özel log formatlarını da destekler.

6. **Binary Loglar Windows Binary Log Dosyaları**: Windows servislerinin ürettiği binary formatlı log dosyalarını okuyabilir. PCAP Dosyaları: Ağ trafiğini temsil eden PCAP dosyalarından log bilgileri çıkarabilir.

Neden .OrianaLOG Tercih Etmeliyim?

1. **Kurulum ve Kullanım Kolaylığı**
   .OrianaLOG kolay kurulum ve kurulum sonrası kullanıcı dostu arayüzü sayesinde kolay ve anlaşılır bir kullanıcı deneyimi sunar. Ayrıca .OrianaLOG'a kaynak ekleme işlemlerini kolaylığı .OrianaLOG kullanıcıları tarafından en önemli tercih sebeplerinden birisi olmuştur.
2. **Düşük Disk Alanı İhtiyacı**
   .OrianaLog veri tekilleştirme algoritması sayesinde tekrarlı verileri tekilleştirme özelliğine sahiptir. Bu sayede disk kullanımında büyük oranda sıkılaştırma yapan nadir LOG-SIEM uygulamasıdır.
3. **Düşük CPU,RAM Tüketimi ve Hızlı Sorgular**
   .OrianaLOG patentli minimize algoritması sayesinde büyük veriler arasında aranan verileri 0.95ms gibi bir sürede getirebilmektedir. Veri sorgu hızının yüksek olması nedeniyle CPU ve RAM tüketimi konusunda ciddi oranda hafif bir kullanım sunar.
4. **Basit SIEM Özelliklerine Sahip Olması**
   .OrianaLOG karmaşık korelasyon mantığını basitleştirerek hızlı, kolay ve anlaşılır bir korelasyon yapısı oluşturmuştur. Bu sayede kullanıcılarına sadece Log Yönetimi ve Merkezileştirme desteği sağlamanın yanında korelasyonlar oluşturarak sistem güvenliğini sağlamayıda hedefler.
5. **Teknolojik Yenilikler**
   .OrianaLOG yeni nesil teknoloji altyapısı ile geliştirilmiştir. Docker, Kubernetes, Multi Platform Languages ve NoSQL veritabanı gibi dağıtımı ve kullanımı kolaylaştıran teknolojiler kullanılmıştır. Bu sayede Kurulum, Versiyon Yükseltme ve Versiyon güncelleme gibi işlemler sırasında kesinti yaşanmamaktadır. Ayrıca bu teknolojiler sayesinde offline sistemlerde bile otomatik sağlık kontrolü mekanizmaları ile sistemde oluşabilecek kesintileri anında tespit edebilmekte ve kendi kendine iyileştirme çalışmaları yapabilmektedir.
6. **Güvenilir Veri Saklama**
   .OrianaLOG sahip olduğu hafif çalışma teknikleri sayesinde sistemler üzerinde en düşük kaynak tüketimini kullanmak üzere şartlanmştır. Bu nedenle sistem kaynaklarını verimli kullanarak gelen verileri sistemi yormadan saklayabilmektedir. Bu sayede veri kaybı yaşanmamaktadır.