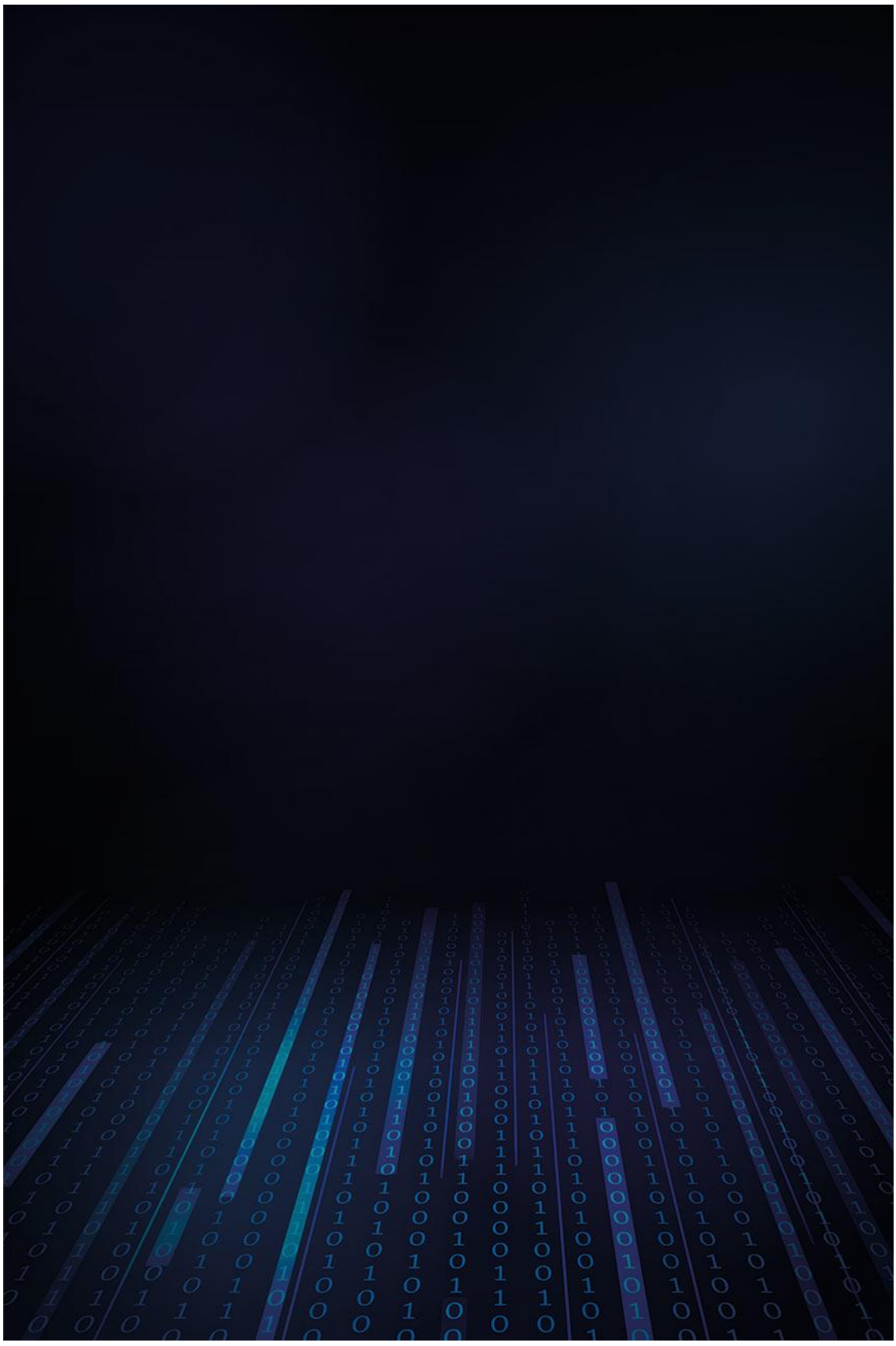
.oriana



.oriana

.OrianaLOG Documentation

.oriana

İçindekiler

Giriş 6

.OrianaLOG Nedir? 6

Kullanım Amacı 6

Yasal Uyumluluk 6

Ürün Özellikleri 7

1. Veri Etiketleme ve Sınıflandırma 7

2. Veri Tekilleştirme (Minimize Algoritması) 7

3. Docker Üzerinde Çalışabilme 7

4. Çeşitli Cihazlardan Veri Toplama 7

5. Bulut Entegrasyonu ve Ölçeklenebilirlik 7

6. Gelişmiş Log Yönetimi ve Analizi 8

7. Yasal Uyumluluk 8

Kurulum Kılavuzu 9

Gereksinimler 9

- İki adet IP Adresi 9

Kurulum Adımları 9

- Ubuntu 22.04 Üzerinde Hazırlık: 9
- .OrianaLOG Kurulumu: 9

.OrianaLOG Kurulum Adımları 9

1. Ana Menü 9
2. .OrianaLOG Kurulumu Başlatma 10
3. İlk IP Adresinin Girilmesi 11
4. Hotspot IP Adresinin Girilmesi 11
5. Alan Adı Girilmesi 12
6. Kurum İsmi Girilmesi 12
7. Firewall Markası Seçilmesi 13
8. SMS Entegrasyonu 14

Kullanım Kılavuzu 16

1. Cihaz Keşfi 16
2. Yeni Bir Cihaz Ekleme 16
3. Cihaz Düzenleme 16

4. Cihaz Loglarını Görüntüleme 16
5. Cihaza Parser Ekleme 16
6. Veri Ambarı Nedir? 16
7. Veri Filtreleme 16
- Zamana Dayalı Veri Filtreleme 16
- Filtreleme Operatörleri 16
8. Log Etiketleri Nedir? 16
9. Etiket Seviyeleri Ne Anlama Gelir? 16
10. Tek Kurallık Korelasyon Nedir? 16
- Bir Cihaza Tek Kurallık Korelasyon Nasıl Eklenir? 16
- Tetiklenen Korelasyonları İnceleme 16
11. Filtre Kısayolları Nedir? 16
12. Eşleşen Veriler Nedir? 16
13. Rapor Oluşturma 16
- Rapor Tasarımları 16
- Ön Tanımlı Rapor Oluşturma 16
- Ön Tanımlı Rapor Kullanımı 16
- Rapor Türleri 17
14. Zaman Damgalı Veri Arşivi 17
- Veri Arşivi İndirme 17
15. Oturum Hareketleri 17
16. Sistem Günlükleri 17
17. İşlem Günlükleri 17
18. Hotspot 17
- Hotspot Entegrasyonları 17
- Hotspota Bağlı Kullanıcılar 17
- Hotspot Oturum Hareketleri 17
- TC Kimlik Numarasını Kara Listeye Ekleme 17
- MAC Adresini Kara Listeye Ekleme 17
- Telefon Numarasını Kara Listeye Ekleme 17
19. Kullanıcılar 17

- MSSP Panel Özellikleri 17
- Kullanıcı Rol Yönetimi 17
- MSSP Kullanıcısına Cihaz Atama 17

20. Cihaz Ayarları 17
- Parser Yapılandırmaları 17
- Cihaz Kolonları 17
- Cihaz Kategorileri 18

21. Lisans Yönetimi 18
22. Zaman Damgası Yönetimi 18
23. Hotspot Oturum Sayfası Tasarımları 18
24. Arşiv Ayarları 18
25. E-Posta Sunucu Ayarları 18
26. SFTP Yapılandırması 18
27. Ajan Yönetimi 18
28. SMS Sağlayıcı Yapılandırması 18
29. Cors Erişim Yapılandırması 18

Log Yönetimi ve Analizi 19

Minimize ve Deduplication Algoritmaları 19

Teknik Destek ve Sıkça Sorulan Sorular (SSS) 20

Neden OrianaLOG? 20

Yanıt Süresi Karşılaştırması 20

Ölçeklenebilirlik Karşılaştırması 20

OrianaLOG'un öne çıkan farklılıkları ve özellikleri nelerdir? 21

OrianaLOG'un veri toplama yetenekleri nelerdir? 21

OrianaLOG'un rekabet avantajları nelerdir? 22

OrianaLOG'un kullanıcı arayüzü nasıldır? 22

Güncellemeler ve İyileştirmeler 23

Ekler 24

.oriana

Giriş

.OrianaLOG Nedir?

.OrianaLOG, dijital dünyada veri güvenliğini sağlamak amacıyla geliştirilmiş yenilikçi bir log yönetim yazılımıdır. Kullanıcıların çeşitli kaynaklardan topladığı verilerin merkezi bir platformda güvenli bir şekilde saklanmasını, analiz edilmesini ve yönetilmesini sağlar. Yazılım, gelişmiş özellikleri sayesinde büyük veri kümeleri üzerinde etkin bir log yönetimi sunarak siber güvenlik tehditlerine karşı etkin bir koruma sağlar.

Kullanım Amacı

.OrianaLOG, kurumların ve işletmelerin, siber güvenlik ve veri yönetimi gereksinimlerini karşılamak amacıyla tasarlanmıştır. Yazılım, logların etkin bir şekilde toplanması, depolanması ve analiz edilmesini sağlayarak veri bütünlüğü ve güvenliği sağlar. Kullanıcılar, .OrianaLOG'u kullanarak güvenlik tehditlerini hızlı bir şekilde tespit edebilir, uyumluluk raporlarını hazırlayabilir ve verilerini güvenli bir şekilde yönetebilirler.

Yasal Uyumluluk

.OrianaLOG, Türkiye'de ve uluslararası alanda geçerli olan yasal düzenlemelere tam uyumluluk sağlar. Yazılım, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5070 sayılı Elektronik İmza Kanunu, Kişisel Verilerin Korunması Kanunu (KVKK) ve Genel Veri Koruma Tüzüğü (GDPR) gibi yasal düzenlemelere uygun olarak geliştirilmiştir. Bu sayede, kullanıcılar .OrianaLOG ile yasal zorunluluklarını kolayca yerine getirebilir ve veri güvenliğini en üst düzeye çıkarabilirler.

.oriana

Ürün Özellikleri

.OrianaLOG, siber güvenlik ve büyük veri yönetimi alanlarında öne çıkan yenilikçi bir log yönetim yazılımıdır. Aşağıda, .OrianaLOG'un sunduğu temel özellikler ve avantajlar detaylı bir şekilde açıklanmıştır.

1. Veri Etiketleme ve Sınıflandırma

.OrianaLOG, toplanan verilerin anlamlı bir şekilde etiketlenmesine ve sınıflandırılmasına olanak tanır. Bu özellik sayesinde kullanıcılar, veri analizi ve raporlama süreçlerini daha verimli bir şekilde gerçekleştirebilir. Verilerin doğru ve tutarlı bir şekilde etiketlenmesi, güvenlik olaylarının daha hızlı ve etkili bir şekilde tespit edilmesini sağlar.

2. Veri Tekilleştirme (Minimize Algoritması)

Yazılım, geliştirilmiş özel bir "Minimize" algoritması kullanarak verilerin depolama alanını en aza indirger. Bu özellik, yinelenen veya aynı verilerin birden fazla kez depolanmasını engeller, disk alanını verimli bir şekilde kullanır ve veri erişim süreçlerini hızlandırır. Bu sayede, büyük veri kümeleri üzerinde maliyetleri düşürürken, veri yönetimini daha etkin hale getirir.

3. Docker Üzerinde Çalışabilme

.OrianaLOG, Docker üzerinde çalışabilme yeteneğine sahiptir. Bu sayede, yazılım hızlı bir şekilde dağıtılabilir ve kullanıcılar tarafından hızla kullanıma başlanabilir. Docker tabanlı altyapı, yazılımın esnekliğini artırır ve işletmelerin operasyonlarına kolayca entegre olmasını sağlar.

4. Çeşitli Cihazlardan Veri Toplama

.OrianaLOG, sunucular, depolama üniteleri, parmak izi okuma sistemleri, anti-virüs yazılımları, veri kaybını önleme (DLP) çözümleri, güvenlik duvarları (firewall) gibi çeşitli cihazlardan gelen verileri toplama yeteneğine sahiptir. Bu veriler, merkezi bir platformda bir araya getirilir ve analiz edilir. Böylece, farklı kaynaklardan gelen verilerin yönetimi ve güvenliği sağlanır.

5. Bulut Entegrasyonu ve Ölçeklenebilirlik

Yazılım, bulut bilişim teknolojileriyle entegre olabilir ve gereksinimlere göre kolayca ölçeklenebilir. Bu özellik, artan veri hacimleriyle başa çıkmak için ideal bir çözüm sunar. Veri hacmindeki artışlar yazılımın performansını etkilemez ve yüksek hızda veri erişimi ve analizi sağlanır. Ayrıca, bulut tabanlı ölçeklenebilirlik, hızlı büyüme durumlarında ek kaynaklara kolayca erişim sağlar ve maliyetleri optimize eder.

6. Gelişmiş Log Yönetimi ve Analizi

.OrianaLOG, log verilerinin etkin bir şekilde toplanması, depolanması ve analiz edilmesi için gelişmiş teknolojik altyapıya sahiptir. Yazılım, çeşitli cihazlardan gelen log verilerini merkezi bir platformda toplayarak kullanıcıların veri güvenliğini sağlamalarına yardımcı olur. Gelişmiş analiz araçları sayesinde, güvenlik olayları hızlı bir şekilde tespit edilir ve uygun aksiyonlar alınabilir.

7. Yasal Uyumluluk

Yazılım, 5651 sayılı Kanun, 5070 sayılı Kanun, KVKK ve GDPR gibi yasal düzenlemelere tam uyumluluk sağlar. Bu özellik, kurumların ve işletmelerin yasal zorunluluklarını yerine getirmelerine yardımcı olur ve veri güvenliğini en üst düzeye çıkarır.

Bu özellikler, .OrianaLOG'u siber güvenlik ve büyük veri yönetimi alanlarında öne çıkan ve tercih edilen bir yazılım haline getirmektedir.

.oriana

Kurulum Kılavuzu

.OrianaLOG yazılımı Docker üzerinde çalışabildiği için Docker kurulu her ortamda kullanılabilir. Ancak, en stabil ve test edilmiş ortam olarak **Ubuntu 22.04** işletim sistemi önerilmektedir.

Gereksinimler

- **İki adet IP Adresi:** .OrianaLOG yazılımı, iki IP adresine ihtiyaç duyar. Bu nedenle, kurulacak cihaz üzerinde iki adet network kartı bulunmalıdır. Bu IP adreslerinden biri **.OrianaLOG** tarafından, diğeri ise **.OrianaSPOT** tarafından kullanılacaktır. Bu düzenleme, her iki uygulamanın birbirinden izole bir şekilde çalışabilmesi için yapılmıştır.

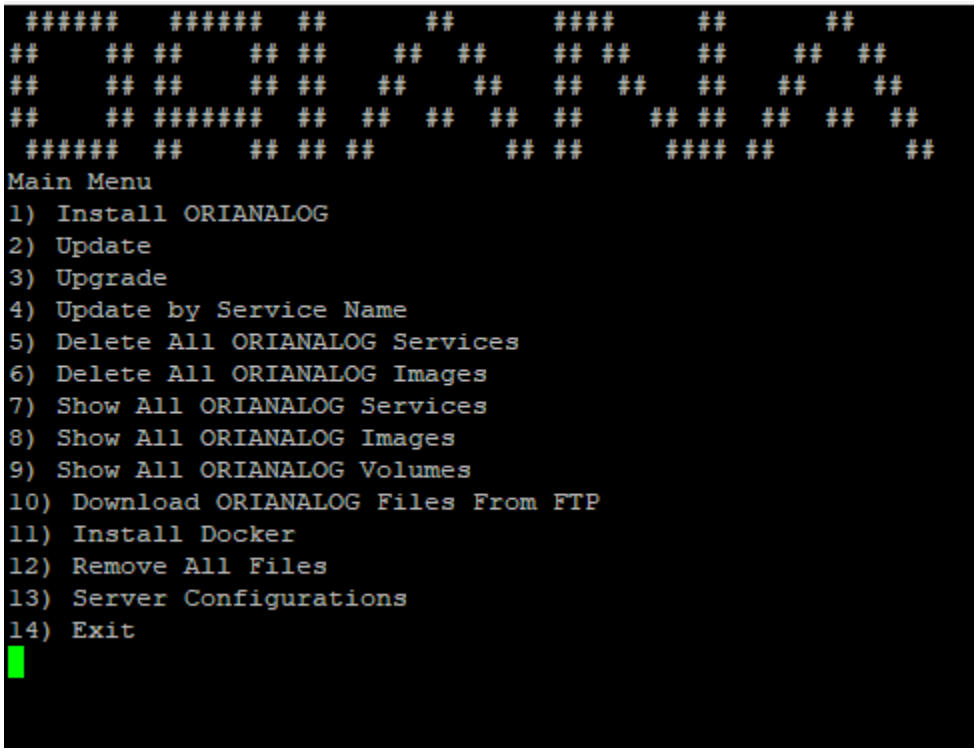
Kurulum Adımları

- Ubuntu 22.04 Üzerinde Hazırlık:
    - Cihazınıza iki adet IP adresi atanmış olduğundan emin olun.
    - Docker ve Docker Compose'un sisteminizde kurulu ve çalışır durumda olduğundan emin olun.
- .OrianaLOG Kurulumu:
    - Docker Compose'un kurulu olduğu ortamda .OrianaLOG kurulum scriptini çalıştırın.
    - Kurulum scripti, gerekli tüm bileşenleri otomatik olarak yapılandıracak ve yazılımın çalışmaya hazır hale gelmesini sağlayacaktır.

Kurulum işlemi tamamlandığında, .OrianaLOG ve .OrianaSPOT, belirtilen IP adresleri üzerinden izole bir şekilde çalışacaktır.

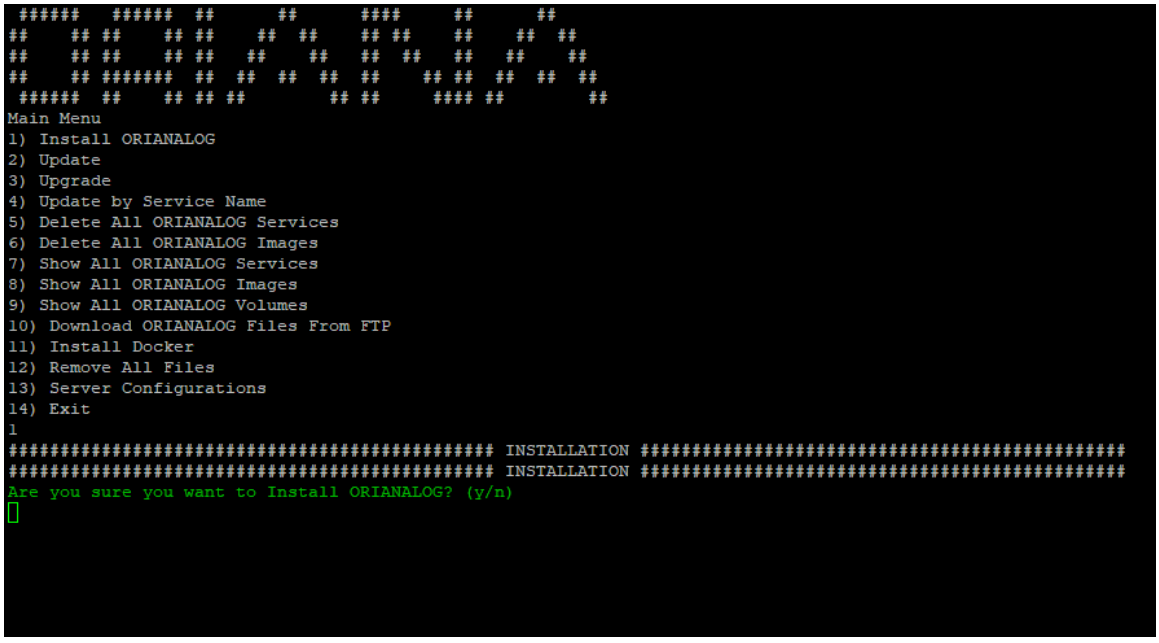
.OrianaLOG Kurulum Adımları

1. **Ana Menü**
    - İlk olarak kurulum scripti çalıştırıldığında **Ana Menü** ekrana gelir. Burada çeşitli seçenekler mevcuttur. .OrianaLOG kurulumu için `1)` seçeneği seçilir



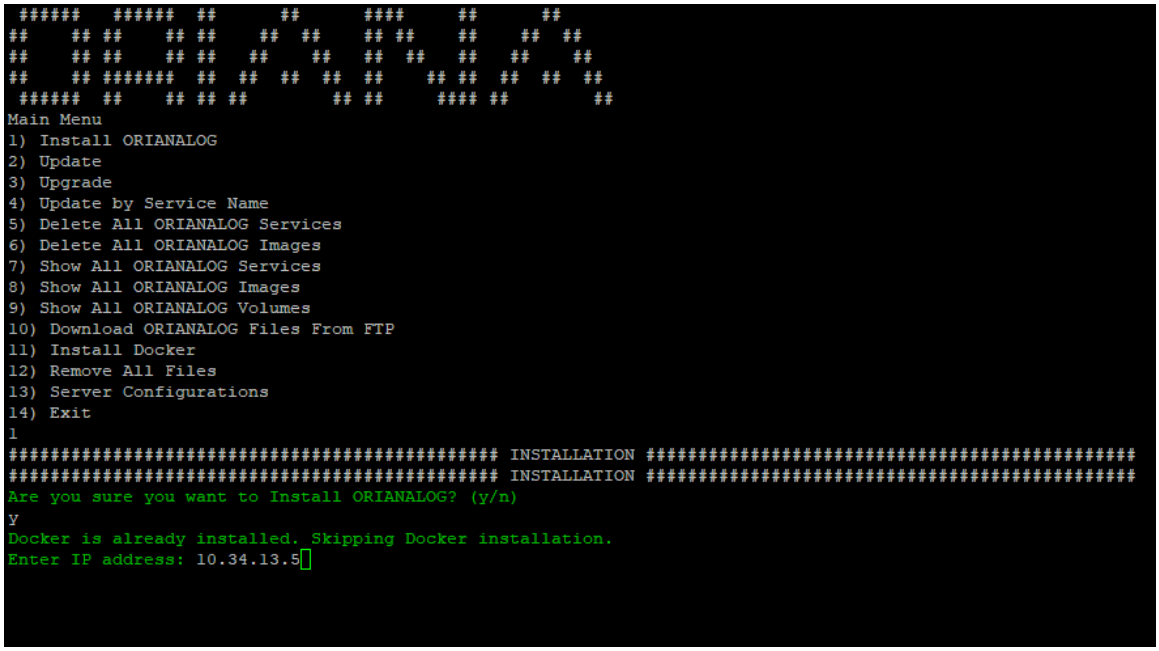
2. .OrianaLOG Kurulumu Başlatma

- `1` seçeneğine basıldığında .OrianaLOG kurulum işlemi başlatılır. Bu aşamada sistem, `.OrianaLOG'u kurmak istiyor musunuz?` sorusunu sorar. "**y**" yazarak devam edilir.



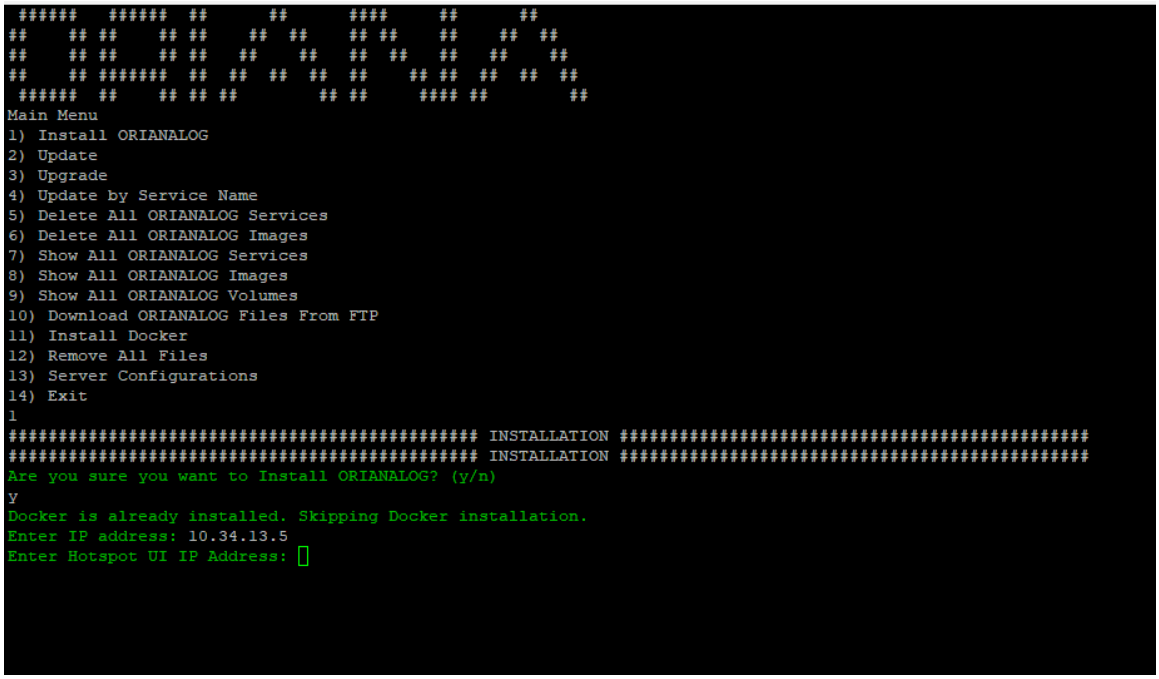
3. İlk IP Adresinin Girilmesi

- Kurulum işlemi sırasında, .OrianaLOG'un kullanacağı ilk IP adresi girilir.



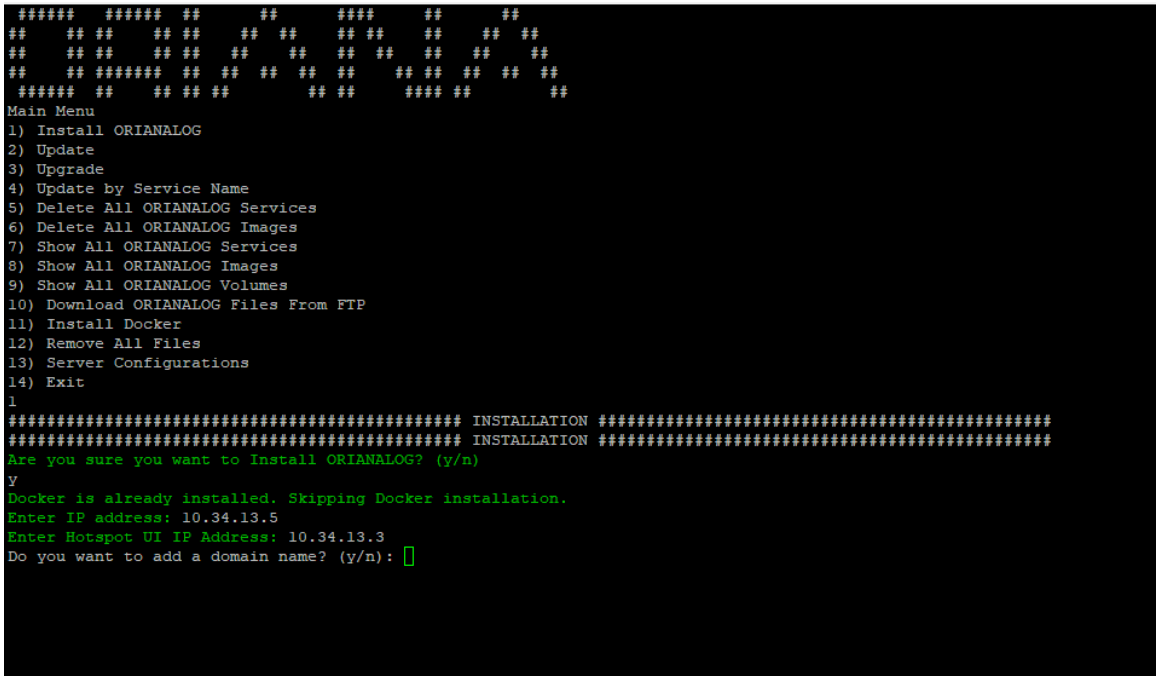
4. Hotspot IP Adresinin Girilmesi

- Hotspot'un kullanacağı ikinci IP adresi girilir. Bu IP adresi .OrianaSPOT tarafından kullanılacaktır.



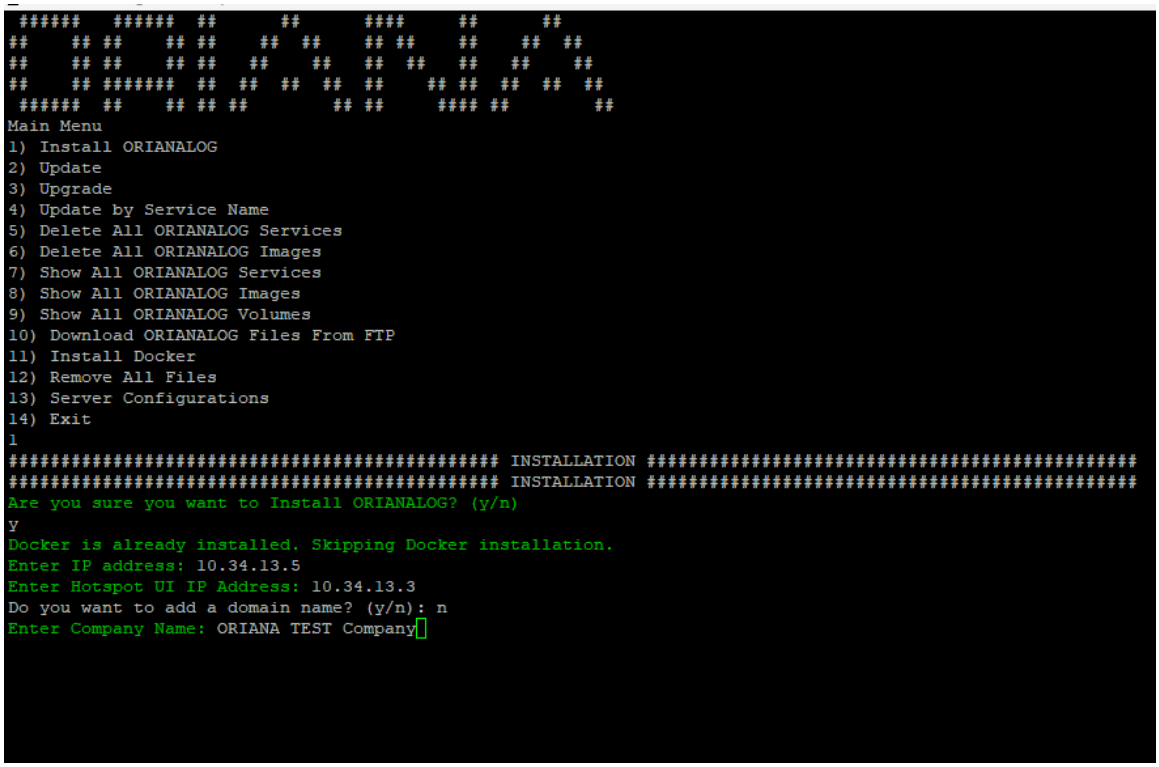
5. Alan Adı Girilmesi

- .OrianaLOG bir alan adı ile kullanılacaksa, bu adımda alan adı girilir. Eğer bir alan adı kullanılmayacaksa **"n"** seçilerek devam edilir.



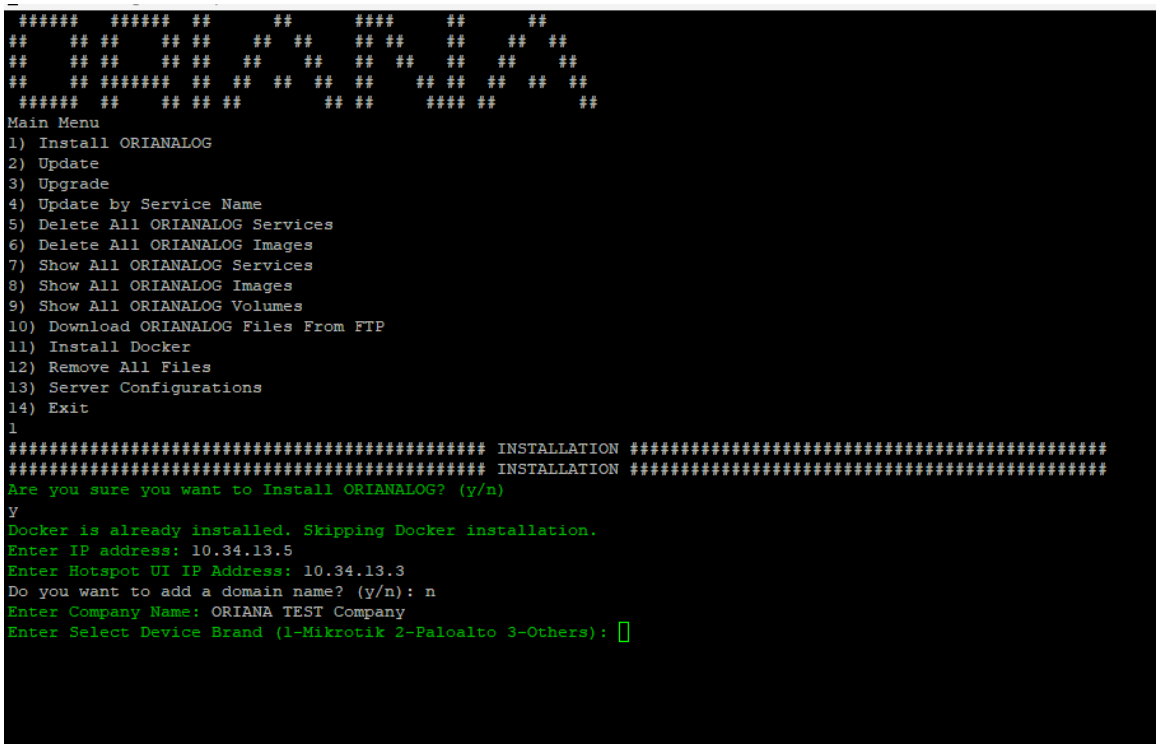
6. Kurum İsmi Girilmesi

- Kurulumun yapıldığı kurumun ismi girilir. Bu bilgi .OrianaLOG'un mail gönderme ve lisanslama işlemleri için kullanılacaktır.



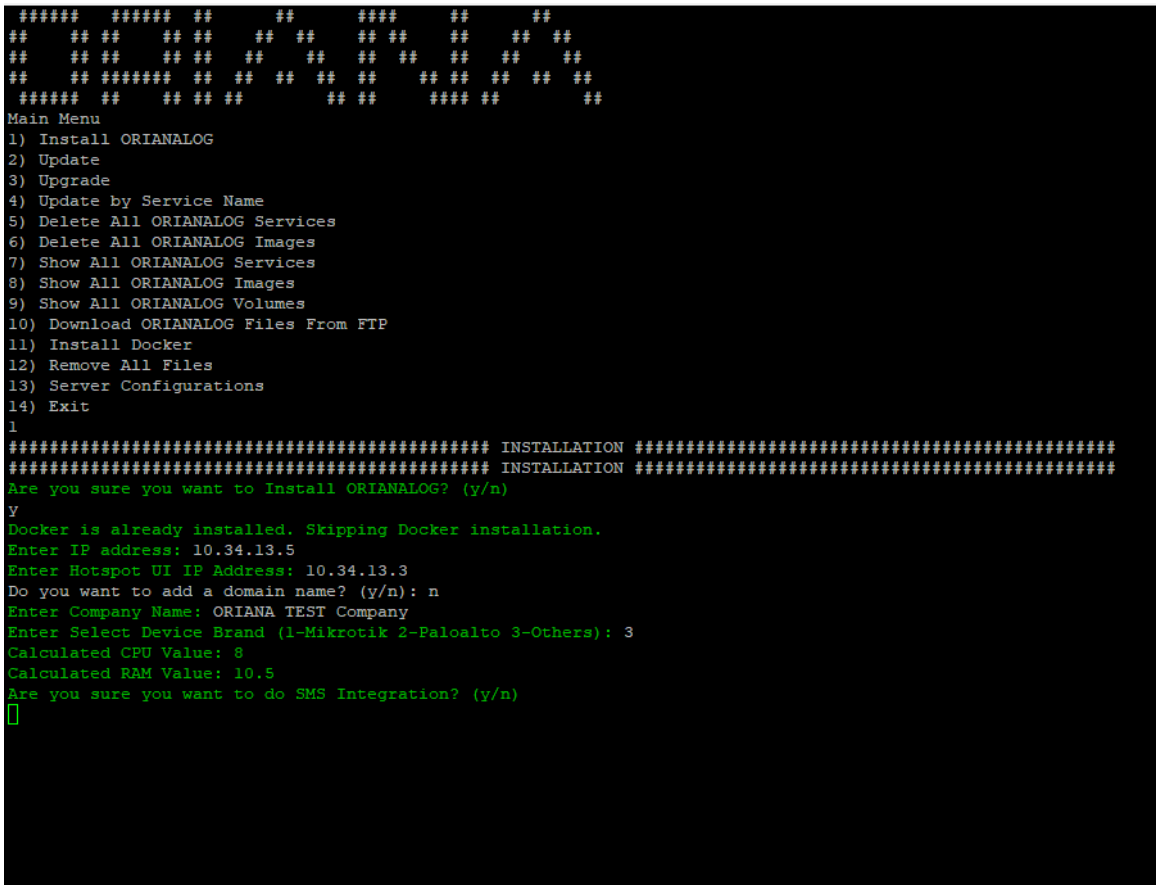
7. Firewall Markası Seçilmesi

- Hotspot uyumluluğu için kurumda bulunan firewall markası seçilmelidir. Bu adımda doğru firewall markası seçimi yapılmalıdır.



8. SMS Entegrasyonu

- NetGSM veya PostaGüvercini hesapları varsa, bu adımda "**y**" seçilerek tanımlama yapılabilir. Ancak, V1.5 versiyonundan sonra bu ayar .OrianaLOG arayüzündeki ayarlar sayfasına taşınmıştır.



Tüm bu adımlardan sonra kurulum işlemi başlatılır. Kurulum süresi internet hızınıza bağlı olarak değişebilir. Kurulum tamamlandıktan sonra, .OrianaLOG arayüzüne `https://serveripaddress` şeklinde erişim sağlayabilirsiniz.

.oriana

Kullanım Kılavuzu

1. Cihaz Keşfi
2. Yeni Bir Cihaz Ekleme
3. Cihaz Düzenleme
4. Cihaz Loglarını Görüntüleme
5. Cihaza Parser Ekleme
6. Veri Ambarı Nedir?
7. Veri Filtreleme
    - Zamana Dayalı Veri Filtreleme
    - Filtreleme Operatörleri
8. Log Etiketleri Nedir?
9. Etiket Seviyeleri Ne Anlama Gelir?
10. Tek Kurallık Korelasyon Nedir?
    - Bir Cihaza Tek Kurallık Korelasyon Nasıl Eklenir?
    - Tetiklenen Korelasyonları İnceleme
11. Filtre Kısayolları Nedir?
12. Eşleşen Veriler Nedir?
13. Rapor Oluşturma
    - Rapor Tasarımları
        - *Statik Rapor Tasarımı Oluşturma*
        - *Dinamik Rapor Tasarımı Oluşturma*
    - Ön Tanımlı Rapor Oluşturma
    - Ön Tanımlı Rapor Kullanımı

- Rapor Türleri
  - *Anlık Rapor*
  - *Günlük Rapor*
  - *Haftalık Rapor*
  - *Aylık Rapor*

14. Zaman Damgalı Veri Arşivi

- Veri Arşivi İndirme

15. Oturum Hareketleri

16. Sistem Günlükleri

17. İşlem Günlükleri

18. Hotspot

- Hotspot Entegrasyonları
- Hotspota Bağlı Kullanıcılar
- Hotspot Oturum Hareketleri
- TC Kimlik Numarasını Kara Listeye Ekleme
- MAC Adresini Kara Listeye Ekleme
- Telefon Numarasını Kara Listeye Ekleme

19. Kullanıcılar

- MSSP Panel Özellikleri
- Kullanıcı Rol Yönetimi
- MSSP Kullanıcısına Cihaz Atama

20. Cihaz Ayarları

- Parser Yapılandırmaları
- Cihaz Kolonları

- Cihaz Kategorileri

21. Lisans Yönetimi

22. Zaman Damgası Yönetimi

23. Hotspot Oturum Sayfası Tasarımları

24. Arşiv Ayarları

25. E-Posta Sunucu Ayarları

26. SFTP Yapılandırması

27. Ajan Yönetimi

28. SMS Sağlayıcı Yapılandırması

29. Cors Erişim Yapılandırması

.oriana

Log Yönetimi ve Analizi

Minimize ve Deduplication Algoritmaları

.OrianaLOG, log yönetimi ve analizi süreçlerini optimize etmek için gelişmiş Minimize ve Deduplication algoritmalarını kullanır. Bu algoritmalar sayesinde, sistemdeki log verilerinin yönetimi ve analizi hem daha hızlı hem de daha verimli bir şekilde gerçekleştirilir.

1. Minimize Algoritması Minimize algoritması, .OrianaLOG'un log verilerini depolarken disk alanını en verimli şekilde kullanmasını sağlar. Bu algoritma, yinelenen verileri tespit eder ve sadece gerekli olan benzersiz verileri saklar. Böylece, büyük veri kümeleri daha az yer kaplar ve maliyetler düşürülür. Ayrıca, verilerin daha küçük bir alanda saklanması, veri erişim ve analiz süreçlerinin hızını artırır. Kullanıcılar, bu algoritma sayesinde log verilerine daha hızlı erişim sağlayabilir ve yüksek performanslı sorgular gerçekleştirebilir.

2. Deduplication Algoritması Deduplication algoritması, .OrianaLOG'un veri tekilleştirme süreçlerini yönetir. Bu algoritma, sistemde yinelenen verilerin birden fazla kez saklanmasını engeller. Tekilleştirilen veriler, disk kullanımını en aza indirgerken, veri yönetimi süreçlerinin etkinliğini artırır. Deduplication sayesinde, büyük veri kümeleri arasında hızlı sorgulamalar yapılabilir ve veri erişimi hızlandırılır.

Hızlı Sorgular ve Veri Erişimi .OrianaLOG'un Minimize ve Deduplication algoritmaları, log verilerine hızlı ve verimli bir şekilde erişilmesini sağlar. Bu algoritmalar, verilerin disk alanında optimize bir şekilde saklanması sayesinde sorgu sürelerini kısaltır. Kullanıcılar, büyük veri kümeleri arasında bile yüksek performanslı sorgular gerçekleştirebilir ve anlık olarak ihtiyaç duydukları verilere ulaşabilir.

Düşük Disk Alanı Kullanımı Bu gelişmiş algoritmalar, verilerin düşük bir disk alanı kullanılarak saklanmasını sağlar. Böylece, işletmeler büyük veri kümelerini daha az maliyetle depolayabilir ve mevcut depolama kaynaklarını daha verimli kullanabilir. Ayrıca, bu özellik, veri yedekleme ve arşivleme süreçlerinde de önemli avantajlar sunar.

.OrianaLOG'un Minimize ve Deduplication algoritmaları, log yönetimi ve analizi süreçlerinde yüksek performans, hızlı veri erişimi ve düşük maliyet sağlamak için tasarlanmıştır. Bu özellikler, .OrianaLOG'u log yönetimi ve siber güvenlik alanlarında güçlü ve yenilikçi bir çözüm haline getirir.

.oriana

Teknik Destek ve Sıkça Sorulan Sorular (SSS)

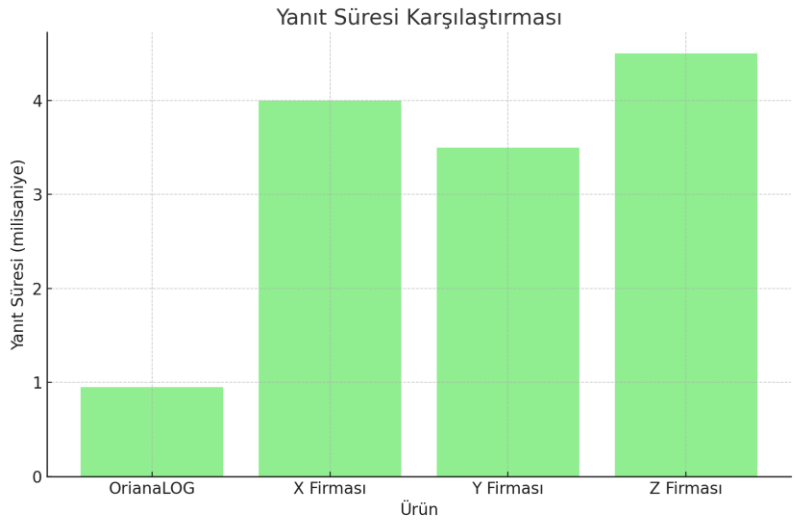
Neden OrianaLOG?

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.

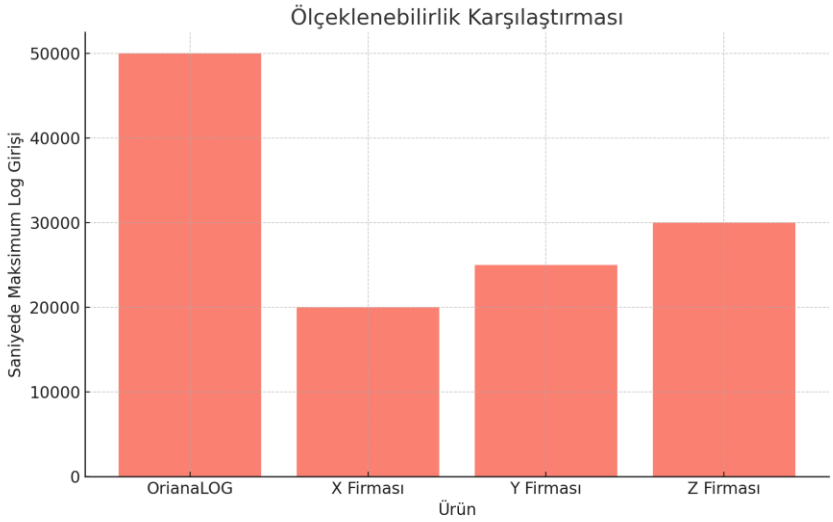
Yanıt Süresi Karşılaştırması

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.

.oriana

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

.oriana

Güncellemeler ve İyileştirmeler

Ekler