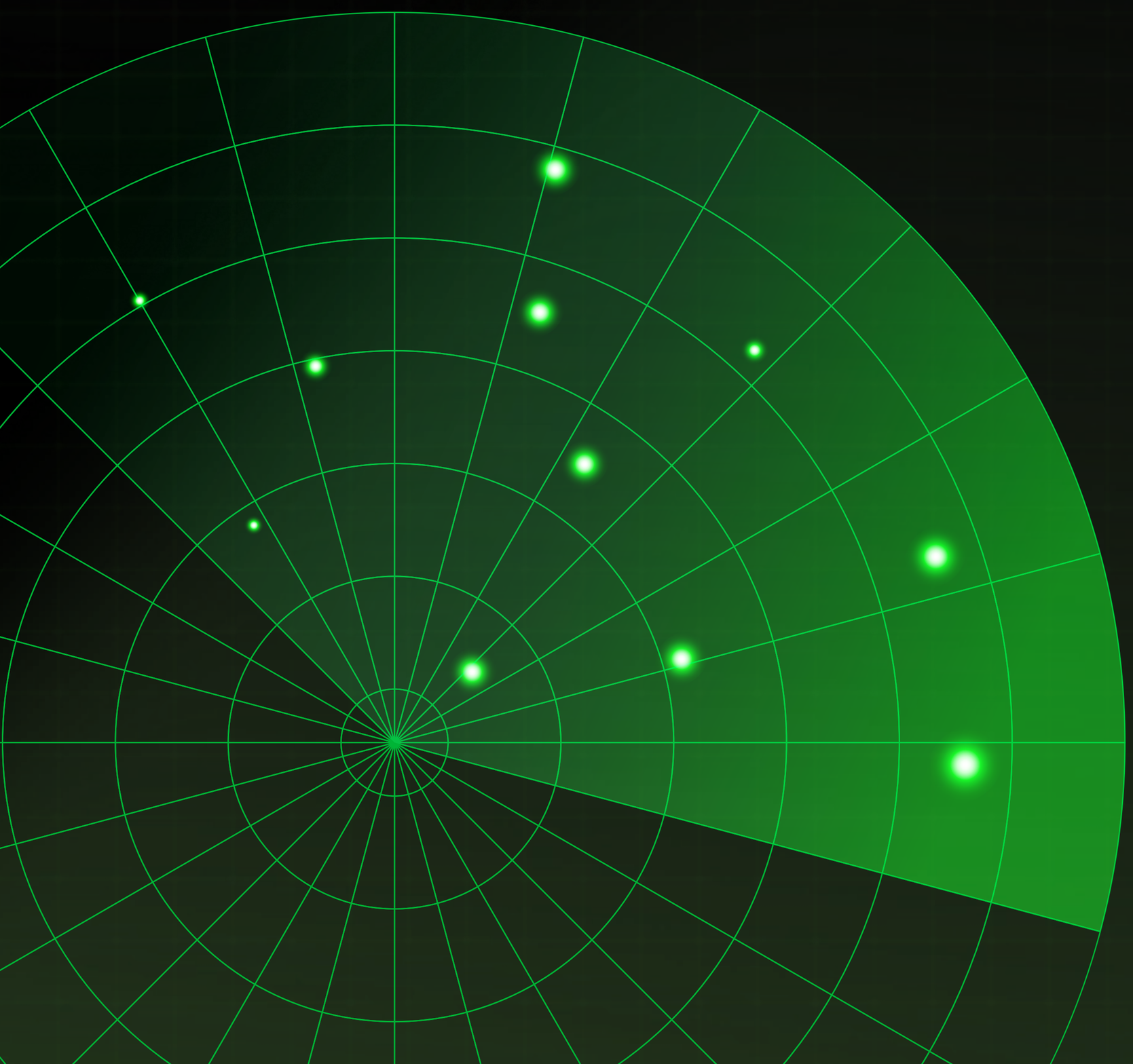
Merkezi Log Yönetimi ve SIEM Platformu

- 5651 ile Tam Uyum
- PCI-DSS standartı ile %100 Uyumlu
- ISO-27001 Sistemi ile Tam Uyumlu
- KVKK ile Uyumlu

Logchase ile tanışmaya hazır mısınız?

Kaosu bir saniyenin altında (<1s) işlenebilir içgörülere dönüştürüyoruz. Log yönetimi artık ekibinizin omuzlarındaki bir yük değil, operasyonel güvenliğinizin ve yasal uyumluluğunuzun sarsılmaz temelidir.



İletişim Bilgilerimiz

+90 (850) 305 88 66

info@logchase.com

www.logchase.com

Ataket Mah. Dicle Cd. No:9/A
Ümraniye/İSTANBUL

8 The Green Suite 13105
Dover, DE, 19901, USA

Siber Güvenlikte YENİ NESİL Kontrol Merkezi

Milyonlarca satır veri arasında kaybolmaya son. Logchase, karmaşık IT altyapınızdaki siber tehditleri saniyeler içinde anlamlandırarak **organizasyonunuzu proaktif bir savunma hattına dönüştürür.**

Neden Logchase?

Kurumsal log yönetimi ve SIEM çözümlerinde fark yaratan özellikler

- Tam Uyumluluk
- Yüksek Performans
- 7/24 Teknik Destek

Logchase, kurumsal log yönetimi ve SIEM ihtiyaçları için merkezi toplama, akıllı alarm sistemleri ve gelişmiş analitik çözümler sunan kapsamlı bir platformdur. KVKK, 5651 ve PCI-DSS gibi yasal standartlara tam uyum sağlayan sistem; cloud veya self-hosted gibi esnek dağıtım seçenekleriyle her ölçekteki işletmeye hitap eder. Güçlü entegrasyon ağı ve "Core"dan "Elite"e uzanan paket seçenekleriyle verilerin güvenliğini ve izlenebilirliğini tek bir noktadan optimize eder.

1M+	50+	99.9%	24/7
Olay/Saniye	Hazır Parser	Uptime SLA	Teknik Destek

logchase

Güçlü Özellikler

Merkezi Log Toplama

Tüm sistemlerinizden gelen logları tek bir merkezde toplayın. Sunucular, ağ cihazları, uygulamalar ve güvenlik sistemlerinden gelen veriler otomatik olarak normalize edilir ve depolanır.

Syslog, API, SFTP, Veritabanı desteği

Gelişmiş Arama & Analitik

Milyonlarca log kaydı içinde saniyeler içinde arama yapın. Güçlü filtreleme, regex desteği ve gerçek zamanlı analitik ile anomalileri hızla tespit ederek organizasyonunuzu proaktif bir savunma hattına dönüştürün.

Saniyede 1M+ olay işleme

Akıllı Alarm Sistemi

Özelleştirilebilir alarm kuralları ile şüpheli aktiviteleri anında tespit edin. E-posta, SMS ve webhook entegrasyonları ile 7/24 bilgilendirme alın.

Korelasyon motoru ile gelişmiş tehdit algılama

Gelişmiş Raporlama

Hazır rapor şablonları ile hızlı başlangıç yapın veya ihtiyacınıza özel raporlar tasarlayın. Zamanlanmış raporlar ile yöneticilerinizi otomatik bilgilendirin.

PDF, Excel export & zamanlama

Bilgi

Görsel, modern IT dünyasında her gün üretilen büyük hacimli log verilerinin geleneksel yöntemlerle yönetilemediğini ve bunun güvenlik riskleri ile uyumluluk sorunlarına yol açtığını anlatıyor. Logchase yaklaşımı ise bu karmaşayı 1 saniyeden kısa sürede anlamlı içgörülere dönüştürerek log yönetimini bir yük olmaktan çıkarıp operasyonel verimlilik ve güvenliğin temel parçası haline getiriyor.

Entegrasyonlar & Ekosistem Mevcut altyapınızla sorunsuz entegrasyon.

Popüler platformlar ve servislerle hazır bağlantılar.

Fortinet · Palo Alto · Cisco · Juniper · MikroTik · pfSense · Sophos · SonicWall

Nginx · Apache · IIS · HAProxy · Traefik · Caddy · MySQL · PostgreSQL · MSSQL

MongoDB · Redis · REST API · Webhook · JSON · Batch Import · Real-time

Windows Event · Linux Syslog · macOS · VMware · Kubernetes · Docker · ForcePoint

McAfee · Trend Micro · WatchGuard · Symantec · CrowdStrike

Log yönetimini bir zorunluluktan çıkarıp gücünüze dönüştürün...

Esnek Dağıtım Seçenekleri

İhtiyacınıza göre ister tam kontrol sağlayan self-hosted,
ister hızlı ve ölçeklenebilir cloud altyapı ile esnek dağıtım seçenekleri sunar.

Self-hosted veya cloud ile esnek kurulum seçenekleri

Self Hosted

Kendi veri merkezinizde tam kontrol ve veri egemenliği.
Güvenlik politikalarınıza tam uyum.

- Anında başlangıç
- Otomatik güncellemeler
- Esnek ölçeklendirme
- Yönetilen altyapı

Cloud

Hızlı kurulum, otomatik güncelleme ve ölçeklenebilir altyapı.
Operasyonel yükü minimuma indirin.

- Anında başlangıç
- Otomatik güncellemeler
- Esnek ölçeklendirme
- Yönetilen altyapı

On-Premise Paket Karşılaştırma

Özellikler	Core	Advanced	Enterprise	Elite
Log Sources	5	5 / 15 / 25 / 50	5 / 15 / 25 / 50	25 / 50 / 100 +
EPS	Sınırsız	Sınırsız	Sınırsız	Sınırsız
Destek Türü	Ticket	Ticket	Ticket&Telefon	Ticket&Telefon
SLA	İş Saatleri	İş Saatleri	24/7	24/7
Sistem Kullanıcıları	1 Kullanıcı	3 Kullanıcı	10 Kullanıcı	Sınırsız
Yetkilendirme (RBAC)	✗	✓	✓	✓
Dashboard	✓	✓	✓	✓
Arama	✓	✓	✓	✓
Raporlama	✗	✓	✓	✓
Log Toplama Yöntemleri	✓	✓	✓	✓
Alarm Yönetim Modülü	✗	✓	✓	✓
Alarm Aksiyonu	✗	✓	✓	✓
Olay Yönetimi Modülü	✗	✓	✓	✓
Risk Puanlama	✗	✓	✓	✓
Custom Parsel	✗	✓	✓	✓
FIM	✗	✗	✓	✓
Threat Intelligence	✗	✗	✓	✓
Disaster Replication	✗	✗	✓	✓
Multi Tenant	✗	✗	2 Tenants	5 Tenants
HA Cluster	✗	✗	3 Nodes	5+ Nodes

Paketler Hakkında Genel Bilgilendirme

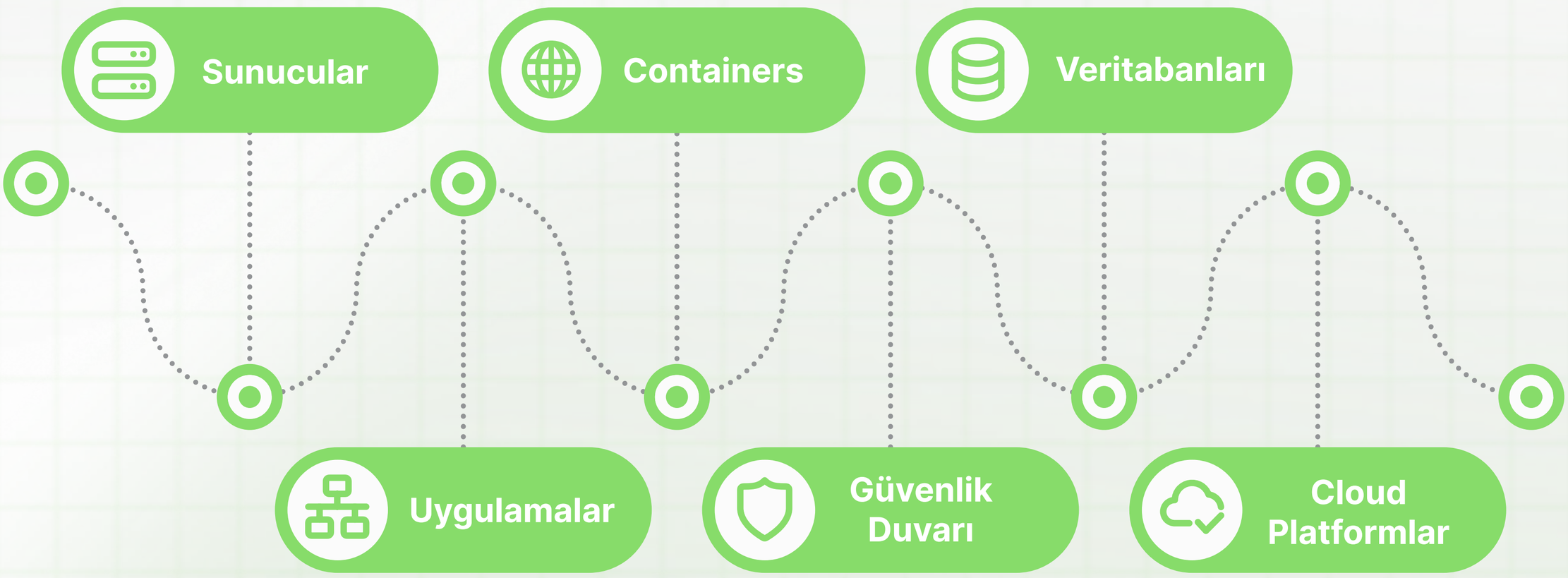
On-Premise paketler, Core'dan Elite seviyesine kadar farklı ihtiyaçlara göre ölçeklenebilir bir yapı sunar. Tüm paketlerde sınırsız EPS ve temel log yönetimi özellikleri bulunurken, üst paketlerde yetkilendirme (RBAC), alarm yönetimi ve olay yönetimi gibi gelişmiş özellikler eklenir. Enterprise ve Elite seviyelerinde FIM, Threat Intelligence ve Disaster Replication gibi kritik güvenlik yetenekleri devreye girer. Ayrıca bu üst paketler, çoklu tenant desteği ve yüksek erişilebilirlik (HA cluster) gibi kurumsal ihtiyaçları karşılar. Destek seviyesi de paketlere göre gelişerek 7/24 hizmete kadar çıkar. Bu yapı sayesinde kurumlar ihtiyaçlarına göre esnek ve kademeli bir geçiş yapabilir.

MERKEZİ Log Management PLATFORMU

Herhangi bir sistemden logları gerçek zamanlı olarak toplayın, normalize edin ve arayın. **Logchase**, sunuculardan, uygulamalardan, ağ cihazlarınızdan ve cloud ortamlardan logları merkezileştirerek hızlı arama, analiz ve sorun giderme imkanı sağlar.

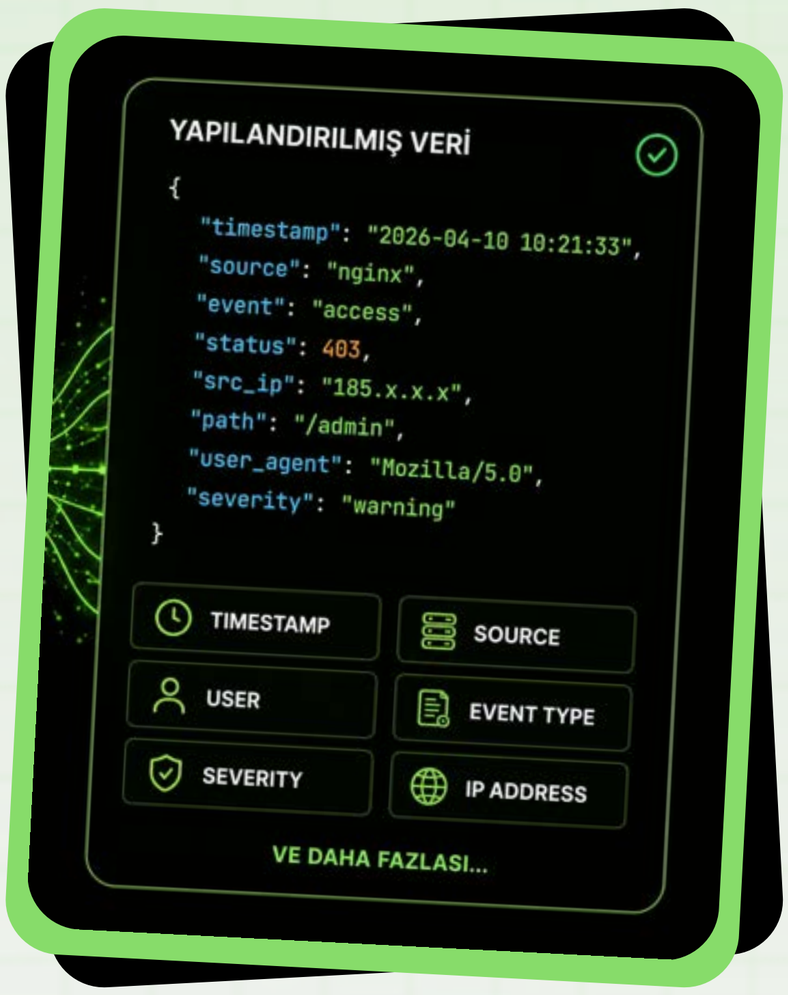
Her Yerden Log Toplayın

Sunucular, uygulamalar, container'lar, güvenlik duvarları, veritabanları ve cloud platformlardan log toplayın.



Desteklenen Yöntemler

- Syslog
- REST API
- File Collectors
- Agents
- SFTP Import
- Database Collectors



Veriyi Otomatik Normalize Edin

Ham logları otomatik olarak anlamlı ve yapılandırılmış veri alanlarına dönüştürerek analiz sürecinizi hızlandırın. Vendor bağımsız parse motoru sayesinde farklı kaynaklardan gelen log formatlarını tek bir standartta birleştirin. 50+ hazır parser ile dakikalar içinde entegrasyon sağlayabilir, timestamp, source, user, event type, severity ve IP address gibi kritik alanları otomatik olarak çıkarabilirsiniz. Böylece manuel işlem yükünü azaltır, hata payını minimuma indirir ve güvenlik, izleme ve raporlama süreçlerinizi çok daha verimli hale getirirsiniz.

- Timestamp
- Event type
- Source
- Severity
- User
- IP address

Log Bütünlüğü Güvencesi

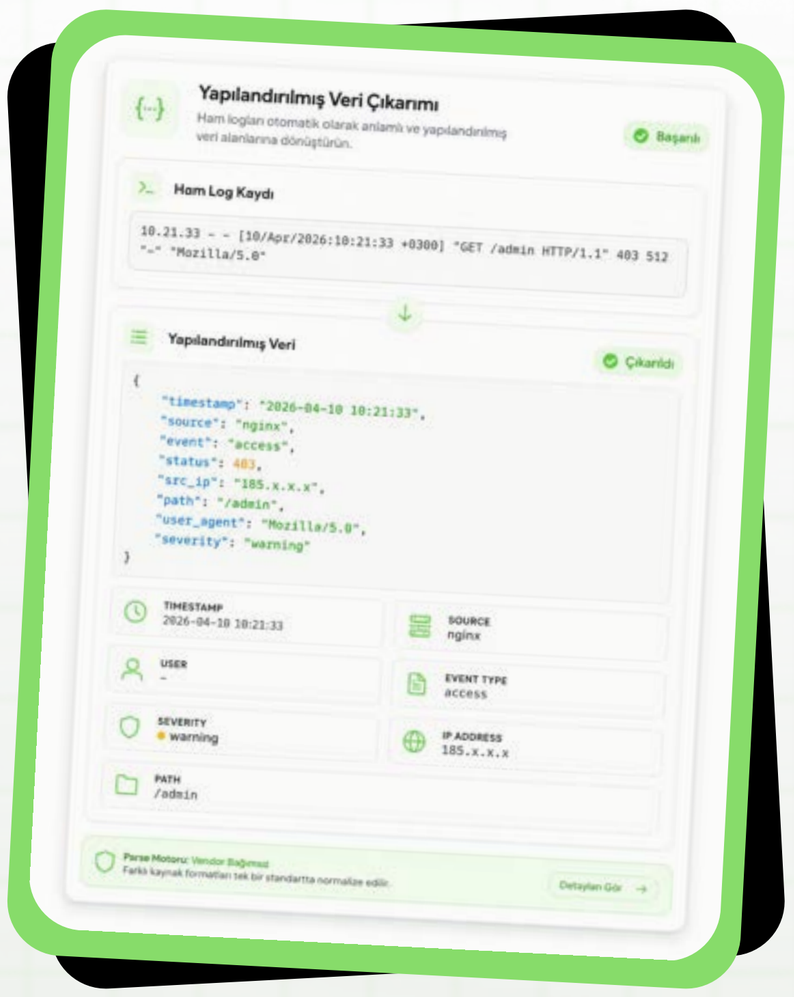
Her log kaydı benzersiz bir kriptografik hash ile korunur ve değiştirilmediği doğrulanabilir. Log arşivleri zaman damgası ile imzalanarak saklanır.

Kriptografik Hash
Her log kaydı SHA-256 hash ile benzersiz şekilde imzalanır.

Zaman Damgası
Log arşivleri FreeSA veya Tübitak Zamane ile imzalanarak saklanır.

Bütünlük Doğrulama
Logların değiştirilip değiştirilmediği her zaman doğrulanabilir.

Yasal Geçerlilik
Değiştirilemez kayıtlar ile yasal süreçlerde geçerli delil niteliği.



Güçlü Arama Motoru

Milyarlarca log kaydı içinde saniyeler içinde arama yapmanızı sağlayan güçlü arama motoru ile ihtiyacınız olan veriye hızlıca ulaşın. Tam metin arama sayesinde tüm içerik üzerinde detaylı sorgular yapabilir, alan bazlı filtreleme ile sonuçları kolayca daraltabilirsiniz. Regex desteği ile karmaşık arama senaryolarını çözebilir, zaman aralığı filtreleme ile belirli dönemlere odaklanabilirsiniz. Kayıtlı sorgular özelliği sayesinde sık kullandığınız aramaları saklayarak analiz süreçlerinizi hızlandırabilirsiniz.

- Tam metin arama
- Zaman aralığı filtreleme
- Alan bazlı filtreleme
- Kayıtlı sorgular
- Regex arama
- Güçlü arama motoru

Felaket Kurtarma

Disaster Recovery Replication

logchase

Felaket kurtarma işlemi nasıl yapılır?

Tüm log verileriniz otomatik olarak coğrafi olarak ayrılmış felaket kurtarma lokasyonuna gerçek zamanlı replike edilir. Veri kaybı riski sıfıra indirilir, kesintisiz iş sürekliliği sağlanır.

Gerçek Zamanlı Replikasyon

Loglar anında felaket kurtarma lokasyonuna senkronize edilir. RPO≈ 0.

Coğrafi Yedeklilik

Farklı coğrafi bölgelerde ayrılmış veri merkezleri ile tam koruma.

Kesintisiz İş Sürekliliği

Felaket senaryolarında bile log toplama ve analiz kesintisiz devam eder.

Gerçek Zamanlı Log Analitik

İstatistiksel analiz ve davranışsal kalıplar ile anomalileri ve örüntüleri tespit edin.

- İstatistiksel analiz
- Davranışsal kalıplar
- Baseline karşılaştırma
- Log frekans analizi

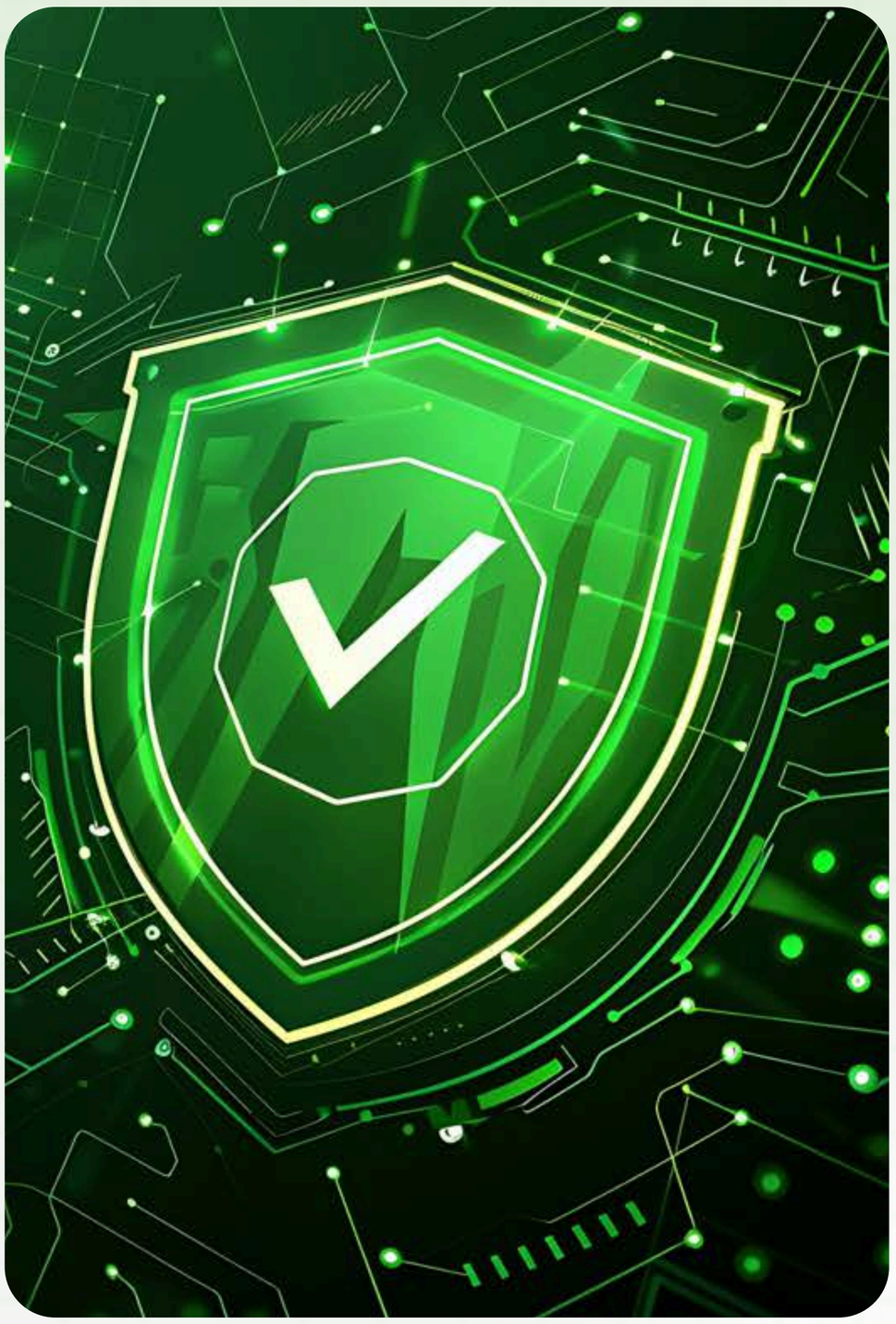
Kullanım Senaryoları

HIZLI VE AKILLI LOG ANALİZİ

Sorunları Hızlı Çözme
Merkezi loglar ile kök nedeni hızlıca bulun.

Denetim ve Uyumluluk
Uyumluluk gereksinimleri için uzun süreli log kayıtlarını saklayın.

DevOps Gözlemlenebilirlik
Uygulama loglarını analiz ederek hataları ve performans sorunlarını tespit edin.



Tehlikeyi büyümeden önce görün ve anında müdahale edin.

Modern Güvenlik Ekipleri İçin SIEM Platformu

Korelasyon Motoru

Birden fazla log kaynağından gelen verileri ilişkilendirerek tekil olayların ötesine geçin. Farklı sistemlerde gerçekleşen aktiviteleri bir araya getirerek saldırı zincirlerini ve anomali kalıplarını tespit edin. Örneğin, aynı IP üzerinden gelen çoklu başarısız giriş denemelerinin ardından gerçekleşen başarılı bir login veya yetki yükseltme gibi kritik senaryoları otomatik olarak ortaya çıkarın.

Merkezi Güvenlik Görünürlüğü

Tüm altyapınızdan gelen logları tek bir noktada toplayarak uçtan uca görünürlük sağlayın. Sunucular, endpoint'ler, uygulamalar ve güvenlik duvarlarından gelen verileri merkezi olarak izleyin. Bu sayede sistemler arası bağlantıları daha net görür, tehditleri daha hızlı fark eder ve müdahale sürecinizi hızlandırırsınız.

Alarm Kuralları ve Algılama Mantığı

Log frekansı, belirli kalıplar ve alan bazlı değerler üzerinden özelleştirilebilir alarm kuralları oluşturun. Anomali algılama ve tehdit istihbaratı eşleşmeleri ile kritik olayları otomatik olarak tespit edin. Örneğin, kısa sürede gerçekleşen brute force denemeleri, beklenmeyen kullanıcı aktiviteleri veya hassas verilere erişim gibi durumlar için anlık uyarılar alın.

1M+	<1S	Gerçek Zamanlı
SANİYEDE OLAY ALIMI	ARAMA PERFORMANSI	ALARM İŞLEME

SOC İş Akışı Desteği

Logchase güvenlik ekiplerinin olayları tespit etmesine, araştırmasına ve hızlı müdahale etmesine yardımcı olur.

Olayları tespit et	Olayları araştır	Alarmları önceliklendir	Hızlı müdahale et
ADIM 1	ADIM 2	ADIM 3	ADIM 4

Modern SIEM platformu, güvenlik ekiplerinin tüm log verilerini tek bir noktada toplamasını, analiz etmesini ve anlamlı içgörülere dönüştürmesini sağlar. Farklı kaynaklardan gelen verileri korelasyon motoru ile ilişkilendirerek saldırı zincirlerini ortaya çıkarır, merkezi görünürlük ile altyapının tamamını izlenebilir hale getirir ve gelişmiş alarm mekanizmaları ile tehditleri anında tespit eder. Bu sayede güvenlik ekipleri olaylara daha hızlı müdahale eder, riskleri proaktif şekilde yönetir ve operasyonel verimliliğini artırır.

SIEM nedir?

Log Correlation + Alert + Investigation

SIEM (Security Information and Event Management), farklı sistemlerden gelen log verilerini merkezi olarak toplayan, ilişkilendiren ve analiz eden bir güvenlik çözümüdür. Log correlation ile olaylar arasındaki bağlantıları ortaya çıkarır, alert mekanizması ile tehditleri anında bildirir ve investigation süreçleriyle güvenlik ekiplerinin olayları hızlıca analiz edip müdahale etmesini sağlar.

Korelasyon Motoru

Birden fazla log kaynağında karmaşık saldırı kalıplarını tespit edin.

- Çoklu başarısız giriş ardından başarılı giriş
- Şüpheli aktivite sonrası yetki yükseltme
- Olağandışı coğrafi giriş kalıpları

Merkezi Güvenlik Görünürlüğü

Tüm altyapınızda tam görünürlük elde edin.

- Sunucular
- Endpoints
- Uygulamalar
- Cloud Ortamlar
- Güvenlik Duvarları

Alarm Kuralları Ve Algılama Mantığı

Olay frekansı, log kalıpları, alan değerleri ve anomali algılama bazlı algılama kuralları oluşturun.

- Olay frekansı
- Log kalıpları
- Alan değerleri
- Anomali algılama
- Tehdit istihbaratı eşleşmesi

LOGCHASE ile sadece depolamayın.
Harekete geçin.

Geleneksel Log Depolama vs Logchase SIEM

Geleneksel

Loglar depolanır ama analiz edilmez.

- Pasif depolama
- Manuel arama
- Korelasyon yok
- Gecikmeli alarm

Logchase SIEM

Loglar analiz edilir, korelasyon kurulur ve zenginleştirilir.

- Aktif analiz
- Anında arama
- Korelasyon motoru
- Gerçek zamanlı alarm

Gerçek Zamanlı Threat Detection Tehdit Algılama

Gerçek zamanlı tehdit algılama ile şüpheli aktiviteleri anında tespit ederek olaylar büyümeden müdahale edin. Gelişmiş analiz ve alarm mekanizmaları sayesinde güvenlik risklerini proaktif şekilde yönetin.

Davranışsal Anomali Algılama

Olağandışı aktivite kalıplarını tespit edin.

- Anormal giriş frekansı
- Olağandışı IP lokasyonları
- Beklenmeyen dosya erişimi
- Yetki kötüye kullanımı

Logchase ile tehditleri gerçek zamanlı olarak tespit ederek güvenlik süreçlerinizi proaktif bir yapıya dönüştürün. Farklı kaynaklardan gelen log verilerini anlık olarak analiz eden sistem, şüpheli aktiviteleri daha olaylar büyümeden ortaya çıkarır ve hızlı aksiyon almanızı sağlar. Böylece olası saldırılar henüz başlangıç aşamasındayken fark edilir ve kritik sistemlerinize zarar vermeden engellenir. Gelişmiş korelasyon, alarm ve analiz yetenekleri sayesinde yalnızca tekil olaylara değil, bu olaylar arasındaki ilişkilere de odaklanabilirsiniz. Bu da daha derin bir görünürlük ve daha doğru tehdit tespiti anlamına gelir. Logchase, güvenlik ekiplerinin üzerindeki manuel yükü azaltırken, hızlı müdahale kabiliyeti kazandırarak operasyonel verimliliği artırır ve kurumunuzun siber güvenlik dayanıklılığını güçlendirir.

Tehdit İstihbaratı Entegrasyonu

Threat.live , AbuseIPDB entegrasyonları ile ile zenginleştirilmiş tehdit verileri.
Logları bilinen kötü amaçlı göstergelerle eşleştirin.

- Kötü amaçlı IP adresleri
- Botnet aktivitesi
- TOR çıkış düğümleri
- Brute force kaynakları

Şüpheli Aktivite Algılama

Şüpheli Aktivite Algılama, brute force saldırıları, yetki yükseltme girişimleri ve lateral movement gibi riskli davranışları erken aşamada tespit ederek hızlı müdahale imkânı sağlar.

BRUTE FORCE SALDIRILARI

Çok sayıda başarısız giriş denemesini analiz ederek brute force saldırılarını erken aşamada tespit edin. Hesap güvenliğini korumak için otomatik uyarılarla hızlı aksiyon alın.

WEBSHELL YÜKLEMELERİ

Sunuculara yüklenen şüpheli script ve dosyaları tespit ederek olası arka kapıları engelleyin. Yetkisiz erişim girişimlerini erkenden fark ederek sistem bütünlüğünü koruyun.

YETKİ YÜKSELTME

Kullanıcıların normal yetki seviyesinin dışına çıkan aktivitelerini izleyerek yetki yükseltme girişimlerini belirleyin. Kritik sistemlere izinsiz erişimi önlemek için anında müdahale edin.

ŞÜPHELİ SÜREÇ YÜRÜTME

Beklenmeyen veya zararlı olabilecek süreçleri analiz ederek anomali davranışlarını ortaya çıkarın. Sistem üzerinde çalışan işlemleri sürekli izleyerek tehditleri erken tespit edin.

LATERAL MOVEMENT GİRİŞİMLERİ

Ağ içinde yatay hareket eden saldırgan aktivitelerini tespit ederek yayılmayı engelleyin. Farklı sistemler arasındaki şüpheli bağlantıları analiz ederek saldırı zincirini kırın.

RİSK Puanlama

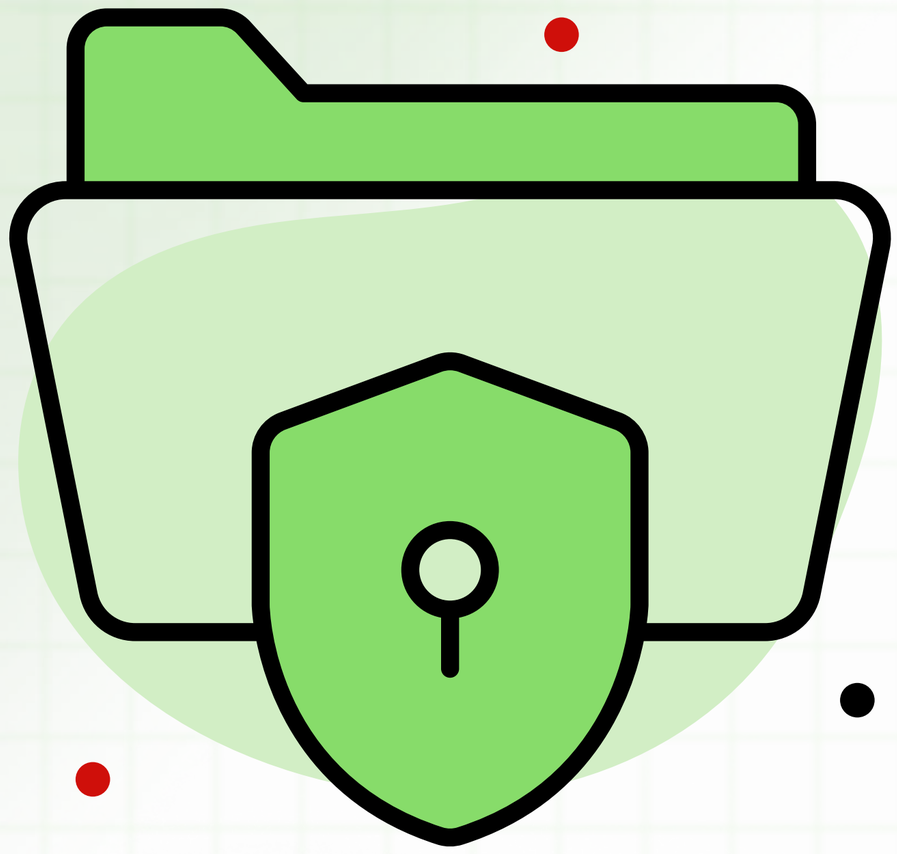
Her olaya risk puanı atanabilir. Soruşturma önceliklendirmesine yardımcı olur.

100-85	84-50	49-25	24-0
KRİTİK	**YÜKSEK**	**ORTA**	**DÜŞÜK**
Aktif saldırı belirtileri	Şüpheli aktivite kalıpları	Bilgi amaçlı olaylar	Bilgi amaçlı olaylar

Logchase, davranışsal anormallik tespiti, tehdit istihbaratı entegrasyonu, şüpheli etkinlik izleme ve risk puanlaması dahil olmak üzere gerçek zamanlı tehdit algılama yetenekleri sunar. Güvenlik ekipleri, altyapıları genelinde kaba kuvvet saldırılarını, webshell dağıtımlarını, ayrıcalık yükseltme girişimlerini ve yatay hareketleri belirleyebilir.

File Integrity FIM Monitoring

Linux ve Windows sunucularınızdaki yetkisiz dosya değişikliklerini gerçek zamanlı olarak tespit edin. **Logchase FIM**, kritik dosya ve dizinleri sürekli izler, yetkisiz değişiklikleri algılar ve olaylar büyümeden güvenlik ekiplerini uyarır.



File Integrity Monitoring (FIM), sistemlerdeki dosya ve dizin değişikliklerini gerçek zamanlı olarak izleyerek güvenliği artıran bir çözümdür. Dosya oluşturma, silme veya değiştirme gibi kritik işlemleri tespit eder ve detaylı şekilde raporlar. Şüpheli değişikliklerde anlık uyarılar oluşturarak hızlı müdahale imkânı sağlar. Ayrıca uyumluluk gereksinimlerini karşılamaya yardımcı olur ve sistem bütünlüğünü sürekli kontrol altında tutar. Bu sayede hem güvenlik hem de denetim süreçleri daha etkin şekilde yönetilir.

File Integrity Monitoring Dosya Bütünlüğü İzleme Nedir?

- Yetkisiz Dosya Değişiklikleri
- Malware / Webshell Dağıtımı
- Ransomware Aktivitesi
- Konfigürasyon Değişiklikleri
- Yetki Yükseltme Girişimleri
- İç Tehditler

Dosya Bütünlüğü İzleme (FIM), dosyalardaki, dizinlerdeki ve sistem yapılandırmalarındaki değişiklikleri algılayan bir güvenlik kontrolüdür. Logchase FIM, hafif ajanlar kullanarak Linux ve Windows sistemlerindeki dosya değişikliklerini gerçek zamanlı görünürlük sağlar.

logchase

FILE INTEGRITY MONITORING TEMEL ÖZELLIKLER

Temel Özellikler Hakkında

Logchase FIM, dosya ve dizinlerdeki tüm değişiklikleri gerçek zamanlı olarak izleyerek neyin, ne zaman ve kim tarafından değiştirildiğini detaylı şekilde gösterir. Esnek izleme kuralları ve akıllı uyarı sistemi sayesinde kritik değişiklikleri anında tespit eder ve hızlı müdahale imkânı sağlar. Hafif ve çapraz platform ajanları ile hem Linux hem Windows ortamlarında yüksek performansla çalışır.

FILE INTEGRITY MONITORING TEMEL ÖZELLIKLER

Gerçek Zamanlı Dosya Değişiklik Algılama

Linux ve Windows sunucularınızdaki kritik dosya ve dizinleri izleyin.

- Dosya oluşturma
- Dosya silme
- İzin değişiklikleri
- Dosya yeniden adlandırma
- İçerik değişikliği
- Hash değişikliği

FILE INTEGRITY MONITORING TEMEL ÖZELLIKLER

Akıllı Uyarı Sistemi

Değişiklik hassasiyetine göre uyarı seviyelerini tanımlayın.

- Dosya yoluna göre
- Dosya türüne göre
- Değişiklik türüne göre
- Hash değişikliğine göre
- Uzantı kurallarına göre
- Kullanıcıya göre

FILE INTEGRITY MONITORING TEMEL ÖZELLIKLER

Detaylı Değişiklik Görünürlüğü

Logchase FIM sadece dosyanın değiştiğini algılamakla kalmaz - tam olarak neyin değiştiğini gösterir.

- Eklenen satırlar
- Silinen satırlar
- Önceki vs yeni hash
- Etkilenen kullanıcı
- Etkilenen süreç
- Değişiklik zaman damgası

FILE INTEGRITY MONITORING TEMEL ÖZELLIKLER

Esnek İzleme Kuralları

Belirli dosyaları, dizinleri, uzantıları veya uygulama kod klasörlerini izleyin.

- /etc
- /var/www
- C:\inetpub
- config files
- scripts
- binaries

FILE INTEGRITY MONITORING TEMEL ÖZELLIKLER

Çapraz Platform Ajanları

Hafif mimari ile minimum performans etkisi. Linux ve Windows desteği.

- Linux sunucular
- Windows sunucular
- Ubuntu sunucular
- Centos sunucular

Kullanım Senaryoları

Logchase FIM, dosya bütünlüğü izlemenin gerekli olduğu birçok güvenlik senaryosunu destekler.

WEBSHELL TESPİTİ

Web dizinlerine yüklenen beklenmeyen PHP, ASPX veya script dosyalarını tespit edin.
/var/www/html/uploads/shell.php

KONFİGÜRASYON DEĞİŞİKLİK İZLEME

Sistem yapılandırma dosyalarındaki değişiklikleri takip edin.
Her türlü uzantıdaki konfigürasyon dosyalarını takip edin.

RANSOMWARE AKTİVİTESI TESPİTİ

Anormal toplu dosya değişikliklerini veya şifreleme kalıplarını tespit edin.

İÇ TEHDİT TESPİTİ

Yetkili kullanıcılar tarafından yapılan izinsiz değişiklikleri takip edin.

UYUMLULUK İZLEME

Dosya izleme gerektiren uyumluluk çerçevelerini destekleyin.
PCI DSS ISO 27001 SOC 2 HIPAA

Dosya oluşturma, silme, değiştirme ve izin değişiklikleri gibi tüm kritik değişiklik türlerini izleyerek sistem bütünlüğünü korur. Hash doğrulama ve kural tabanlı izleme sayesinde dosya değişikliklerini güvenilir şekilde analiz eder ve esnek politikalarla kontrol sağlar.

Desteklenen Değişiklik Türleri

- File created
- File deleted
- File modified
- File renamed
- Permission changed
- Hash changed
- Ownership changed

FILE INTEGRITY MONITORING TEKNİK ÖZELLİKLER

Hash Doğrulama

Kriptografik hash algoritmalarıyla dosya bütünlüğünü doğrulayarak yetkisiz değişiklikleri hızlıca tespit edin. SHA-256 ile güvenli analiz yapın, eski yöntemleri destekleyerek uyumluluğu koruyun.

- SHA-256
- SHA-1
- MD5

FILE INTEGRITY MONITORING TEKNİK ÖZELLİKLER

Kural Tabanlı İzleme

Dizin, uzantı ve hassasiyet seviyesine göre özelleştirilebilir kurallar oluşturarak izleme kapsamını belirleyin. Ortama özel politikalarla kritik dosyaları izleyin ve değişiklikleri kontrol altında tutun.

- Dizin bazlı
- Uzantı bazlı
- Hassasiyet seviyesi
- Ortam bazlı

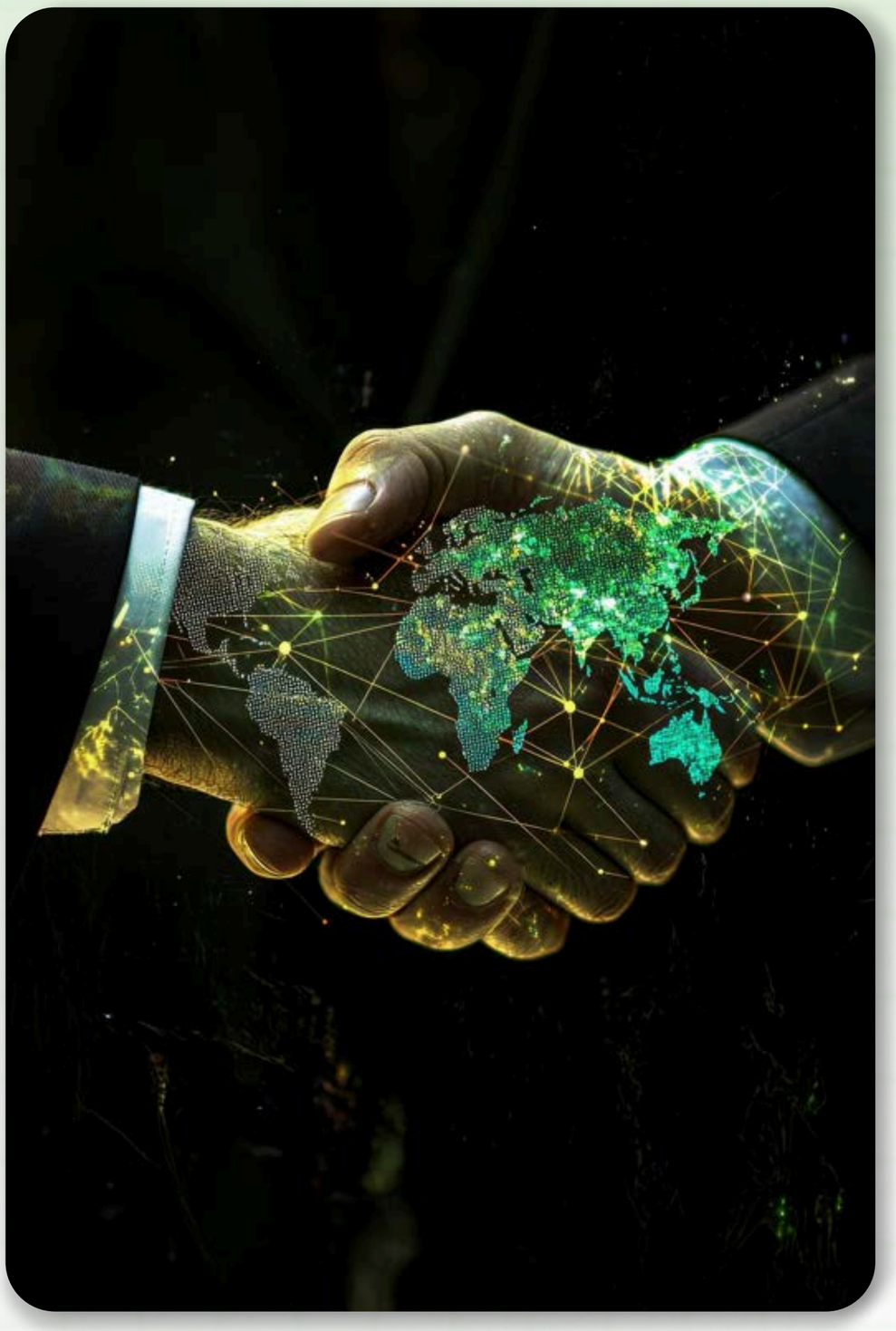
FIM, sistemdeki kritik dosyaları sürekli izleyerek yetkisiz değişiklikleri görünür hale getirir ve güvenlik ekiplerine anında kontrol sağlar. Esnek kural yapısı ve detaylı değişiklik analizi sayesinde hem güvenlik hem de uyumluluk süreçlerini tek platformdan yönetmeyi mümkün kılar. Ayrıca hafif ajan mimarisi ile farklı ortamlarda minimum performans etkisiyle çalışır.

Akıllı Alarm Seviyeleri

Değişiklik hassasiyetine göre alarm seviyelerini otomatik tanımlayın.

Kritik sistem dosyası değişikliği	Kritik sistem dosyası değişikliği	Uygulama konfigürasyon değişikliği	Log dosyası değişikliği
KRİTİK	**YÜKSEK**	**ORTA**	**DÜŞÜK**
/etc/passwd, /etc/shadow	/etc/passwd, /etc/shadow	nginx.conf, web.config	/var/log/*, application logs

Akıllı alarm seviyeleri, dosya değişikliklerini hassasiyetine göre otomatik olarak sınıflandırarak kritik olaylara öncelik verir. Bu sayede güvenlik ekipleri önemli tehditlere hızlıca odaklanırken düşük öneme sahip değişiklikleri kolayca ayırt edebilir.



Neden?

Logchase Partner

Cazip Kar Marjları
Rekabetçi partner indirimleri ve yüksek kar marjları ile işinizi büyütün.

Kapsamlı Eğitim
Satış ve teknik eğitim programları ile ekibinizi Logchase uzmanı yapın.

Teknik Destek
Ön satış ve satış sonrası süreçlerde tam teknik destek alın.

Pazarlama Desteği
Ortak pazarlama faaliyetleri, kampanyalar ve müşteri referanslan.

Lead Paylaşımı
Bölgenizdeki potansiyel müşterileri sizinle paylaşıyoruz.

Sertifikasyon
Resmi Logchase Partner sertifikası ve marka kullanım hakkı

1.Adım
Web sitemizden ön başvuru formunu doldurun.

2.Adım
Ön başvurunuz kabul edildikten sonra satış ekibimiz sizlerle bir görüşme gerçekleştirecektir.

3.Adım
Görüşmenin ardından başvuru sürecinizi tamamlamak için Logchase ekibi iletişime geçecektir.

4.Adım
Partner programına kabul edildikten sonra eğitim ve sertifikasyon sürecini başarıyla tamamlamanız gerekmektedir.

5.Adım
Eğitim ve sertifikasyon sürecini başarıyla tamamladıktan sonra, artık resmi bayimiz olacaksınız.

QR Kodu Tarayarak Başvuru Sayfasına Erişebilirsiniz.

Merkezi Log Yönetimi ve SIEM Platformu

Logchase ile neler başarabileceğinizi kısaca özetledik. Detaylı bilgi almak için bize ulaşabilirsiniz.

Logchase, log yönetimi, SIEM, tehdit algılama ve FIM gibi kritik güvenlik ihtiyaçlarını tek platformda birleştirerek kurumlara uçtan uca görünürlük sağlar. Gerçek zamanlı analiz, güçlü korelasyon ve gelişmiş arama yetenekleri sayesinde güvenlik ekipleri olayları hızlıca tespit edip müdahale edebilir. Esnek yapı, geniş entegrasyon desteği ve farklı dağıtım seçenekleri ile her ölçekten organizasyona kolayca uyum sağlar. Aynı zamanda uyumluluk gereksinimlerini karşılayarak denetim süreçlerini kolaylaştırır. Tüm bu özellikler, güvenlik operasyonlarını daha hızlı, daha verimli ve daha etkili hale getirir.

- Kritik Verilerinizin Muhafızı
- Gerçek Zamanlı SOC İş Akışı
- Kullanıma Hazır Algılama Mantığı
- Aktif Korelasyon Motoru

İletişim Bilgilerimiz

+90 (850) 305 88 66

info@logchase.com

www.logchase.com

Ataket Mah. Dicle Cd. No:9/A
Ümraniye/İSTANBUL

8 The Green Suite 13105
Dover, DE, 19901, USA