DAHA GÜVENLİ YARINLAR İÇİN

Güvenlik görünürlüğü, karar hızına dönüşür.

LogDefence; farklı kaynaklardan gelen güvenlik sinyallerini tek bir operasyon merkezinde toplar, anlamlandırır ve analistin doğru aksiyona daha hızlı ulaşmasını sağlar.

- Birleşik görünürlük
- Gerçek zamanlı operasyon
- Doğrulanmış dayanıklılık



DERİNLEMESİNE ÜRÜN SUNUMU

SIEM Appliance | Satış öncesi tanıtım

NEDEN LOGDEFENCE?

Daha az gürültü. Daha net öncelik.

Dağınık güvenlik sinyallerini tek bir operatör deneyiminde birleştirir.

Ortak görünürlük

Kaynak, olay, alarm, varlık ve sistem sağlığı aynı operasyon diliyle izlenir.

Analist hızı

Filtreleme, zaman çizgisi, bağlam ve aksiyonlar araştırma süresini kısaltır.

Doğru öncelik

Korelasyon, önem ve kaynak bağlamı gerçek riski öne taşır.

Operasyon güveni

Bütünlük, sağlık, karantina ve kapasite göstergeleri sistem davranışını görünür kılar.

Güvenlik operasyonunun dört sorusuna tek ekrandan yanıt

Ne oldu? Nerede oldu? Ne kadar önemli? Sıradaki doğru aksiyon ne?

OPERASYON MERKEZİ

Anlık durumu tek bakışta okuyun

KPI'lar, olay akışı, alarm önceliği, kaynak sağlığı ve servis görünürlüğü aynı çalışma yüzeyinde.



Canlı bağlam

Zaman aralığına göre olay hacmi, EPS, alarm önceliği ve kaynak aktivitesi.

Operatör sağlığı

Toplama, algılama, depolama ve arayüz durumunu anlaşılır sağlık göstergeleriyle izleme.

ARAŞTIRMA AKIŞI

Sinyalden kanıta, bağlam kaybetmeden

Canlı SOC ve olay inceleme ekranları, analistin odağını koruyan ortak filtre ve zaman yaklaşımını kullanır.

Çoklu filtre
Kaynak, parser, IP, önem ve mesaj koşullarını birlikte uygulayın.

Hızlı daraltma
Zaman aralığını değiştirin, sıralayın ve kayıtlı görünümleri tekrar çağırın.

Olay bağlamı
Normalize alanları, kaynak bilgisini ve ilişkili aksiyonları tek yerde görün.

Tutarlı deneyim
Koyu/açık tema ve Türkçe/İngilizce kullanım seçenekleriyle ortak ürün dili.



İLİŞKİLERİ GÖRÜNÜR KILIN

Alarm üretmekten fazlası

Kural, politika ve korelasyon katmanları güvenlik sinyallerini öncelikli bir analist iş akışına dönüştürür.

01
Sinyal
Farklı kaynaklardan gelen olaylar ortak şemada anlam kazanır.

02
Bağlam
Kaynak, varlık, kullanıcı, ağ ve zaman ilişkileri birleştirilir.

03
Algılama
Kural ve politika eşleşmeleri gürültüyü azaltacak biçimde değerlendirilir.

04
Korelasyon
Dağınık işaretler tek bir güvenlik hikâyesinde ilişkilendirilir.

05
Vaka
Alarm; sahiplik, durum, not ve kanıtla yönetilebilir işe dönüşür.

Sonuç: daha az ekran geçişi, daha açık öncelik ve denetlenebilir müdahale izi.

HER KAYNAĞIN DURUMU GÖRÜNÜR

Onboarding'den sürekli sağlığa

Firewall, Windows, Linux ve uygulama kaynakları; kayıt, parser eşleşmesi ve sağlık bağlamıyla yönetilir.

Rehberli onboarding

Kaynak türüne göre yönlendirilmiş kurulum ve doğrulama adımları.

Kaynak doğruluğu

Beklenen parser, kimlik ve akış sağlığını tek görünümde izleme.

Varlık bağlamı

Sinyali yalnız IP olarak değil, iş bağlamı olan varlık olarak ele alma.



YÜK ALTINDA GÜVEN VEREN DAVRANIŞ

Kapasite, yalnız hız değil; veri bütünlüğüdür

Kontrollü lab doğrulamalarında sürekli yük, burst ve bütünlük kapıları birlikte değerlendirildi.

Maksimum performans

1.500 EPS

8 core CPU ve 16 GB RAM ile maksimum performans, sürdürülebilir çalışma.

Ölçülen burst

2.000 EPS

Çok kaynaklı testlerde ölçülen burst performansı.

Olay hacmi

18,78 M

Tek çalışma boyunca kabul edilen olay hacmi.

Veri kaybı

0

Sustained, burst ve cooldown boyunca ölçülen drop.

Operasyonel yaklaşım

Kapasite profili; olay karması, korelasyon yoğunluğu, saklama politikası ve donanım boyutuna göre belirlenir. LogDefence, sağlık ve kaynak göstergeleriyle kapasiteyi görünür kılar; büyüme kararını ölçüme dayandırır.

Değerler kontrollü lab koşullarında ölçülmüştür; üretim boyutlandırması keşif ve kapasite profiliyle yapılır.

BUGÜN DEĞER ÜRETİR, YARINA HAZIRLANIR

Kurulumdan olgun güvenlik operasyonuna

LogDefence; hızlı devreye alma, görünür operasyon ve ölçülebilir büyüme ekseninde konumlanır.

Bugün

- Birleşik dashboard ve Canlı SOC
- Olay, alarm ve vaka iş akışı
- Kaynak ve parser yönetimi
- Kural/politika/korelasyon
- Raporlama ve operatör sağlığı

Yakın dönem kapsamı

- Hazır entegrasyon kataloğunun genişlemesi
- Kanıt paketi ve yönetici raporlarının zenginleşmesi
- Varlık ilişkileri ve saldırı yüzeyi görünürlüğünün derinleşmesi

Kurumsal değer

- Daha hızlı araştırma
- Daha açık öncelik
- Daha güvenilir veri akışı
- Daha kolay işletim
- Ölçülebilir kapasite

Güvenlik verinizi, operasyonel avantaja dönüştürün.

LogDefence keşif, pilot ve kapasite profiliyle kurumunuza uyarlanır.