SOFTBYT LABS

Logdefence Edge

Merkezi görünürlük. Kontrollü veri. Hızlı müdahale.

Logdefence Edge; sunucular, ağ cihazları, güvenlik ürünleri ve uygulamalardan gelen logları kurumun kendi altyapısında toplayan, anlamlandıran ve güvenlik operasyonuna dönüştüren yerinde kurulumlu bir SIEM platformudur.

VERİ KONTROLÜ

Loglar kurumun belirlediği altyapıda kalır.

MERKEZİ İZLEME

Farklı kaynaklar tek operasyon görünümünde birleşir.

GÜVENLİ ANALİZ

Ham veri korunurken olaylar normalize edilerek incelenir.

PLATFORM

Loglardan güvenlik görünürlüğüne

Logdefence Edge, ham olayın toplanmasından araştırma ve alarm sürecine kadar temel SIEM iş akışını tek platformda birleştirir.

Kaynaklar — Toplama — Parser ve Normalizasyon — Detection ve İnceleme

Merkezi log toplama

Sunucu, ağ, güvenlik ve uygulama kaynaklarından gelen olayları ortak bir noktada toplar.

Parser Studio ve Shadow

Bilinen formatları normalize eder; bilinmeyen veya eksik tanımlı formatların kontrollü biçimde incelenmesini ve yeni parser adaylarının oluşturulmasını destekler.

Arama ve olay inceleme

Güvenlik ekiplerinin olayları kaynak, kullanıcı, cihaz, zaman ve diğer alanlar üzerinden araştırmasına yardımcı olur.

Detection ve alarm yönetimi

Normalize edilen olayların güvenlik kurallarıyla değerlendirilmesini ve anlamlı bulgulara dönüştürülmesini sağlar.

Ham veri bütünlüğü

Orijinal logun korunmasını, izlenebilirliğini ve doğrulama zincirleriyle güvenli arşivlenmesini destekler.

Yetkili merkezi yönetim

Kaynak, kullanıcı ve operasyon süreçlerinin merkezi arayüzden rol tabanlı şekilde yönetilmesini sağlar.

KURUMSAL DEĞER

Güvenlik ekipleri için daha net bir çalışma alanı

Logdefence Edge yalnızca log saklamak için değil; farklı sistemlerde dağılmış olayları ilişkilendirilebilir, aranabilir ve operasyonel hale getirmek için tasarlanmıştır.

1

Görünürlük
Dağınık log kaynaklarını tek merkezde izleyerek olayların bütününü görmeye yardımcı olur.

2

Daha hızlı araştırma
Ham ve normalize edilmiş veriyi birlikte koruyarak güvenlik incelemelerinin izlenebilirliğini artırır.

3

Kontrollü öğrenme
Bilinmeyen log biçimlerini ayrı bir öğrenme sürecine alır; yeni parserların kontrollü biçimde geliştirilmesini destekler.

4

Veri egemenliği
Yerinde kurulum yaklaşımıyla kurumun güvenlik verisini ve saklama politikasını kendi kontrolünde tutmasına yardımcı olur.

Kimler için?

Güvenlik operasyonlarını merkezileştirmek, kritik logları kendi altyapısında tutmak ve olay inceleme süreçlerini geliştirmek isteyen kurumlar için.

Kurulum yaklaşımı

Kurumun ölçeğine ve saklama ihtiyacına göre tek sistem veya ayrıştırılmış bileşenlerle, merkezi yönetim yaklaşımıyla konumlandırılabilir.