LOG YÖNETİMİ VE SIEM

Logdefence Edge

Sinyalleriniz.
Daha net bir güvenlik görünümü.

Altyapınızdan gelen logları güvenlik izleme, araştırma ve müdahale için ortak bir görünümde birleştirin.

BİR BAKIŞTA

01 Merkezî log toplama

02 Ayrıştırma ve normalleştirme

03 Tespit ve olay inceleme

04 Ham veri bütünlüğü

Kurulum boyutu ve entegrasyon kapsamı; kaynak biçimleri, olay hacmi, saklama ihtiyacı ve altyapıya göre değerlendirilir.

YETENEKLER VE İŞ AKIŞI

Ham olaylardan kullanılabilir güvenlik bağlamına.

01 ## Altyapı genelinde toplayın

Sunucu, ağ, güvenlik ve uygulama olaylarını ortak bir toplama noktasında birleştirin.

02 ## Biçimleri kullanılabilir hâle getirin

Bilinen biçimleri normalleştirin; bilinmeyenleri Parser Studio ve kontrollü öğrenme süreciyle inceleyin.

03 ## Bağlamla araştırın

Kaynak, cihaz, kullanıcı, zaman ve olay alanlarıyla arayın; normalleştirilen olayları güvenlik kurallarıyla değerlendirin.

04 ## Kanıtı koruyun

Orijinal logların izlenebilirliğini ve bütünlük kontrollerini, rol tabanlı merkezî yönetimle birlikte destekleyin.

Log kaynakları

Toplama

Ayrıştırma ve normalleştirme

Tespit ve inceleme

KULLANIM ALANLARI VE KURULUM

Toplamayı altyapınıza göre kapsamlandırın.

Güvenlik operasyonları	Olayları, alarmları ve kaynak sağlığını ortak bir inceleme iş akışında buluşturun.
Veri kontrolü	Güvenlik loglarını kurumunuzun belirlediği altyapıda tutun.
Bilinmeyen log biçimleri	Tanımlanmamış biçimleri inceleyin; ayrıştırıcı adaylarını kontrollü süreçte geliştirin.

Entegrasyon alanları: Windows ve Linux · Ağ ve güvenlik duvarı logları · Güvenlik ürünleri · Uygulama logları

Kaynak uyumluluğu keşif sırasında kontrol edilir. Ayrıştırma, toplama yöntemi ve kapasite gerçek kaynak ve kurulum profiline bağlıdır.

info@softbytlabs.com