Tespit paketi

Güncel tehdit kayıtlarından tespit içeriği hazırlar.

İŞLEME SINIRI
Açık kaynak akışlarından beslenir

SİTENİN AMACI

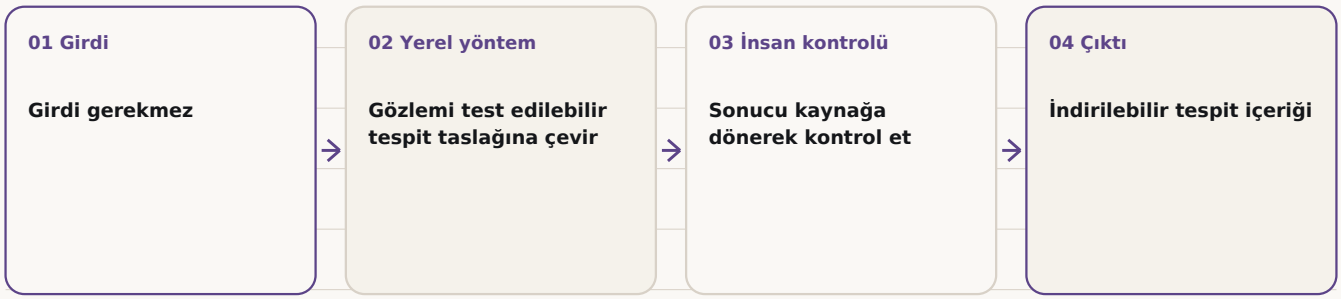
Bu site, bir soruyu güvenli ve tekrar edilebilir bir araştırma sürecine çevirmek için var. Araç sonucu tek başına hüküm değildir; kaynak ve insan kontrolü her zaman görünür kalır.

NEDEN YAPTIM?

Bir CTI kaydını doğrudan kural diye kopyalamak yerine gözlem, mantık, veri gereksinimi ve test notunu aynı pakette tutmak için yaptım.

KÜÇÜK MİMARİ

Girdiden saklanabilir çıktıya dört parça



Tespit paketi

ADIM ADIM KULLANIM

Adım 1

Malzemeyi hazırla

Başlangıçta gereken şey: Girdi gerekmez

Adım 2

Gözlemi test edilebilir tespit taslağına çevir

Güncel tehdit kayıtlarından tespit içeriği hazırlar.

Adım 3

Sonucu kaynağa dönerek kontrol et

Alan adlarını kendi log şemanla eşleştir ve kuralı sentetik veya onaylı geçmiş veriyle dene. Test edilmemiş taslağı üretime alma.

Adım 4

Kaydı indir ve sakla

İnceleme sonunda saklanacak şey: İndirilebilir tespit içeriği

DÜRÜST SINIR

Çıktı tespit taslağıdır. Her SIEM'e hazır değildir, yanlış pozitif oranını bilmez ve otomatik engelleme kararı vermez.