

IOC sorgulama

Bir göstergeyi açık kaynaklardaki kayıtlarla karşılaştırır.

İŞLEME SINIRI

Sorgu sunucu üzerinden yapılır

SİTENİN AMACI

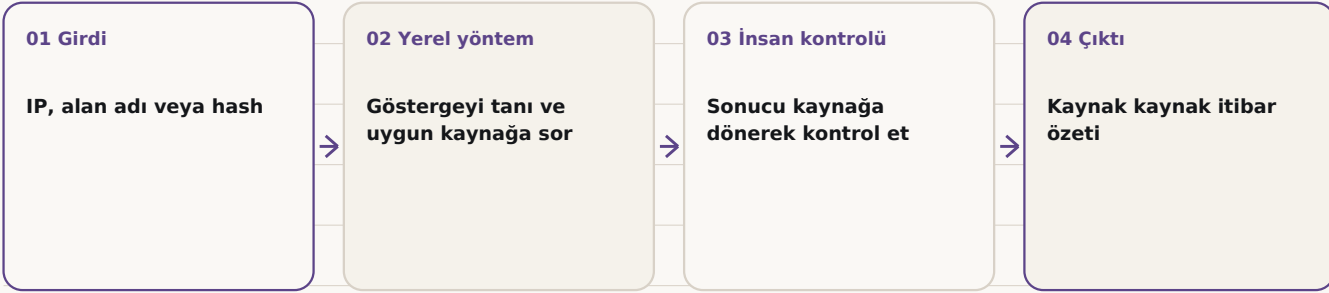
Bu site, bir soruyu güvenli ve tekrar edilebilir bir araştırma sürecine çevirmek için var. Araç sonucu tek başına hüküm değildir; kaynak ve insan kontrolü her zaman görünür kalır.

NEDEN YAPTIM?

Bir IP, domain, URL veya hash hakkında farklı açık kaynak kayıtlarını tek yerde karşılaştırmak ve kaynak tarihini kaybetmemek için yaptım.

KÜÇÜK MİMARİ

Girdiden saklanabilir çıktıya dört parça



IOC sorgulama

ADIM ADIM KULLANIM

Adım 1

Malzemeyi hazırla

Başlangıçta gereken şey: IP, alan adı veya hash

Adım 2

Göstergeyi tanı ve uygun kaynağa sor

Bir göstergeyi açık kaynaklardaki kayıtlarla karşılaştırır.

Adım 3

Sonucu kaynağa dönerek kontrol et

Eşleşmenin tarihini, gösterge türünü ve kaynak açıklamasını kontrol et. Eski veya paylaşımlı bir IP kaydını güncel saldırgan kimliği gibi okuma.

Adım 4

Kaydı indir ve sakla

İnceleme sonunda saklanacak şey: Kaynak kaynak itibar özeti

DÜRÜST SINIR

Kaynaklarda eşleşme bulunmaması göstergenin temiz olduğunu kanıtlamaz. Eşleşme de tek başına olay bağlamını açıklamaz.