

Vaka korelasyon masası

Olay ve varlık kayıtları arasındaki ilişkileri kurar.

İŞLEME SINIRI

Cihazında, tarayıcıda işlenir

SİTENİN AMACI

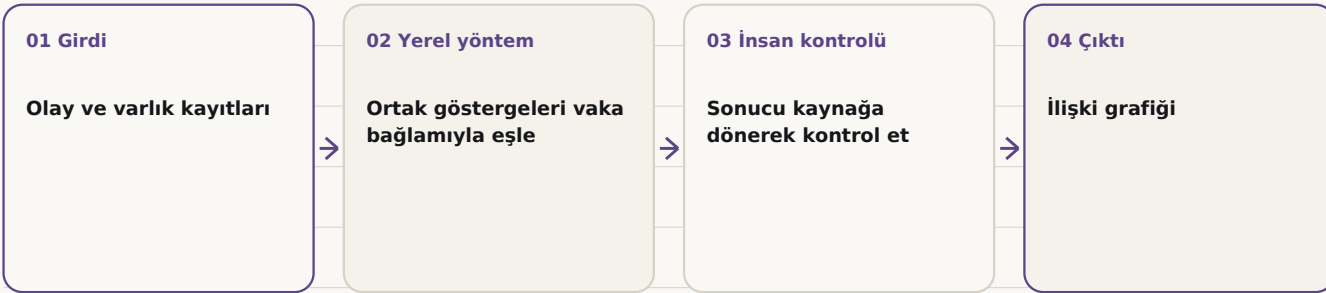
Bu site, bir soruyu güvenli ve tekrar edilebilir bir araştırma sürecine çevirmek için var. Araç sonucu tek başına hüküm değildir; kaynak ve insan kontrolü her zaman görünür kalır.

NEDEN YAPTIM?

Farklı vakalardaki ortak domain, hash veya olayları ilişkilendirirken benzerlik ile kanıtlanmış bağı birbirinden ayırmak için yaptım.

KÜÇÜK MİMARİ

Girdiden saklanabilir çıktıya dört parça



Vaka korelasyon masası

ADIM ADIM KULLANIM

Adım 1

Malzemeyi hazırla

Başlangıçta gereken şey: Olay ve varlık kayıtları

Adım 2

Ortak göstergeleri vaka bağlamıyla eşle

Olay ve varlık kayıtları arasındaki ilişkileri kurar.

Adım 3

Sonucu kaynağa dönerek kontrol et

Her bağlantının iki taraftaki kaynak kaydını ve zaman aralığını kontrol et. Paylaşımlı altyapı veya yaygın araç kullanımını aktör bağı sayma.

Adım 4

Kaydı indir ve sakla

İnceleme sonunda saklanacak şey: İlişki grafiği

DÜRÜST SINIR

Korelasyon bir araştırma ipucudur. Kimlik, nedensellik, aynı kampanya veya saldırgan atfını tek başına kanıtlamaz.