CSINT Incident Lab

Incident Lab, kurgusal ve sanitize edilmiş olay dosyalarıyla kaynak doğrulama, zaman çizelgesi ve raporlama pratiği sunar.

VERİ NEREDE İŞLENİR?
Cihazında çalışır

HEDEF

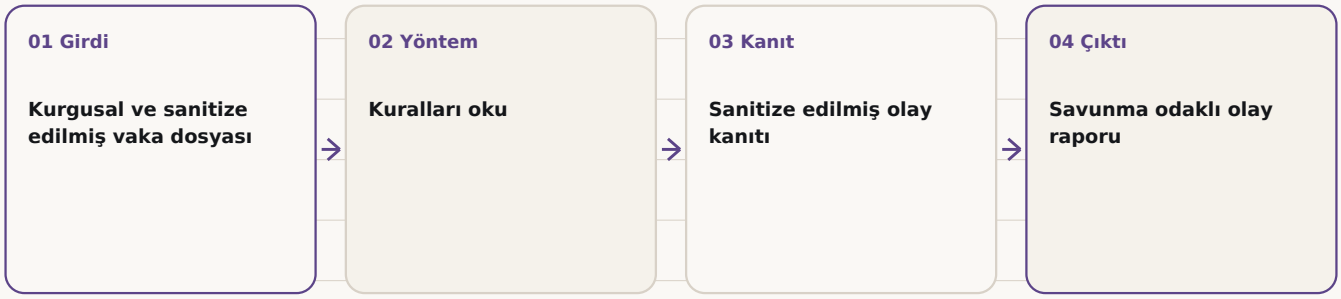
Kurgusal ve sanitize edilmiş kanıtlarla olay analizi ve savunma raporlama pratiği sağlar.

KİM İÇİN?

Kurgusal ve sanitize edilmiş kanıtlarla kaynak doğrulama ve olay analizi pratiği yapmak isteyenler içindir.

TEKNİK AKIŞ

Girdi, yöntem, kanıt ve çıktı



CSINT Incident Lab

NASIL ÇALIŞIR?

Adım 1

Vakayı seç

Seviyene ve öğrenmek istediğin yönteme uygun bir kurgusal vaka seç.

Adım 2

Kuralları oku

Vakanın eğitim sınırını, kullanılacak sanitize edilmiş veriyi ve yasak eylemleri önce kontrol et.

Adım 3

Kanıtları incele

E-posta, zaman damgası, ağ kaydı veya olay notu gibi parçaları kaynaklarıyla birlikte oku.

Adım 4

Zaman çizelgesi kur

Doğrulanan olayları sırala; varsayım ve boşlukları ayrı tut.

Adım 5

Kanıt gücünü değerlendir

Her sonucun hangi kayda dayandığını ve hangi kontrolün hâlâ eksik olduğunu yaz.

Adım 6

Savunma raporu yaz

Bulguyu, belirsizliği ve güvenli savunma önerisini kısa bir raporda birleştir.

SINIRLAR

Lab gerçek kişi, mağdur, canlı hedef veya sızdırılmış veri içermez. İzinsiz erişim, kişi takibi veya canlı sistem testi için kullanılmaz.