Operation Glass Harbor

Operation Glass Harbor, farklı kanıt türlerini tek olay zaman çizelgesinde birleştiren 12 aşamalı kurgusal savunma laboratuvarıdır.

VERİ NEREDE İŞLENİR?
Cihazında çalışır

HEDEF

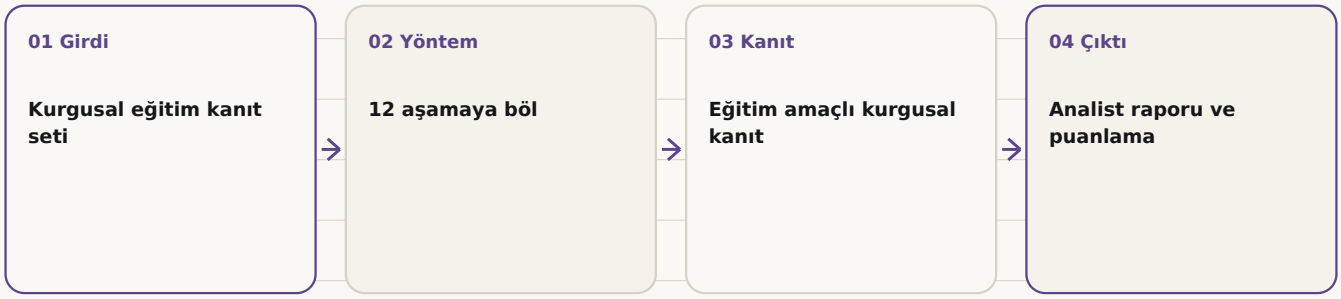
Kurgusal bir kanıt seti üzerinde adım adım analist pratiği sağlar.

KİM İÇİN?

Farklı kanıt türlerini güvenli ve tamamen kurgusal bir olayda adım adım birleştirme pratiği yapmak isteyenler içindir.

TEKNİK AKIŞ

Girdi, yöntem, kanıt ve çıktı



Operation Glass Harbor

NASIL ÇALIŞIR?

Adım 1

Kurgusal kanıt setini hazırla

E-posta, Git, TLS, DNS, görsel, HUMINT, telemetri ve supply-chain dosyaları kaynak yollarıyla birlikte depoda tutulur.

Adım 2

12 aşamaya böl

Her aşama bir soruya, kanıt grubuna, beklenen yönteme ve kontrollü flag değerine bağlanır.

Adım 3

İlerlemeyi yerelde tut

Aşama durumu ve analist notları bu cihazda saklanır; kullanıcı çalışmaya kaldığı yerden devam eder.

Adım 4

Kanıt kaydını puanla

Sistem yalnız doğru cevap yerine kaynak, yöntem ve asgari kanıt kaydının tamamlanmasını da kontrol eder.

Adım 5

Flag'i sunucuda doğrula

Gönderilen flag düz doğru cevap listesiyle değil, sunucu tarafındaki HMAC doğrulamasıyla kontrol edilir.

Adım 6

Analist raporu üret

Tamamlanan aşamalar; zaman çizelgesi, hipotez, kanıt gücü, boşluklar ve savunma önerileri olarak birleştirilir.

SINIRLAR

Bütün kişiler, kurumlar ve olaylar kurgusaldır. Laboratuvar savunma eğitimi içindir; gerçek hedef veya credential içermez.