

USE CASE

Replay an attack path across your architecture

Aribot plays an attack chain step by step across your architecture, labelling each move with its MITRE ATT&CK technique and the component it reaches.

THE PROBLEM

Our threat model lists threats one at a time and never shows how they chain together. Nobody can say which component an attacker reaches after the first foothold. We find out during an incident.

HOW ARIBOT HANDLES IT

- 1 **Start from the architecture**
The simulation runs on a diagram of your client, gateway, services and databases.
- 2 **Play the chain**
Each step moves from one component to the next, tagged with a MITRE ATT&CK technique and phase.
- 3 **Watch the compromise spread**
Components the attacker reaches are marked as compromised as the chain advances.
- 4 **Review the chain**
The full chain is listed, from initial access to impact.

WHAT YOU SEE IN THE DEMO

- An animated attack path from an attacker node through the gateway to services and databases
- Step cards with technique IDs and phases such as Initial Access, Credential Access and Impact
- Play, pause and reset controls
- An attack progress panel counting compromised components and completed steps

WHO IT IS FOR

CISO

Security Architect

SOC Lead

WHAT YOU GET

- Attack paths drawn on your own architecture
- A MITRE ATT&CK technique and phase on every step
- A view of which components an attacker could reach
- Input for choosing the controls that break the chain

20%

of breaches had an exploited vulnerability as the entry point, up 34%

Source: Verizon DBIR 2025

See it: ayurak.com/demos/attack-simulation

€150 per war-game / path-to-green