

USE CASE

Threat intelligence mapped to the systems you run

Aribot joins MITRE ATT&CK techniques and CVE data to the components and resources you have connected, so a new threat shows which systems it reaches.

THE PROBLEM

Our threat feeds are full of campaigns and CVEs, and most have nothing to do with what we run. Working out which ones touch our systems is manual, so it happens late. By the time we know a technique reaches us, the window to act has passed.

HOW ARIBOT HANDLES IT

- 1 **Collect intelligence**
Entries come from MITRE ATT&CK, CVE and NVD data, your cloud accounts and your repositories.
- 2 **Map to your components**
Each technique or CVE is joined to the components and resources it could reach.
- 3 **Track CVE status**
Affected CVEs are tracked as active, mitigated or patched.
- 4 **Feed the threat model**
Mapped threats land on the architecture, next to the controls that stop them.

WHAT YOU SEE IN THE DEMO

- A threat feed with entries tagged by source, including MITRE ATT&CK, CVE / NVD, your cloud accounts and your repositories
- An active CVE table with severity scores and active, mitigated or patched status
- A breakdown of top attack vectors
- A global threat map

WHO IT IS FOR

CISO

Security Architect

SOC Lead

WHAT YOU GET

- Threat intelligence filtered to what you run
- CVE status tracked against affected components
- Threats placed on the architecture with their controls
- A starting point for attack simulation on new techniques

20%

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

Source: Verizon DBIR 2025

See it: ayurak.com/demos/global-intelligence

€150 per war-game / path-to-green