

Raiders of the Lost Architecture

Security Testing in Modern Application

Kevin Tackett
kevin@secureideas.com
904-403-8024
@secureideas

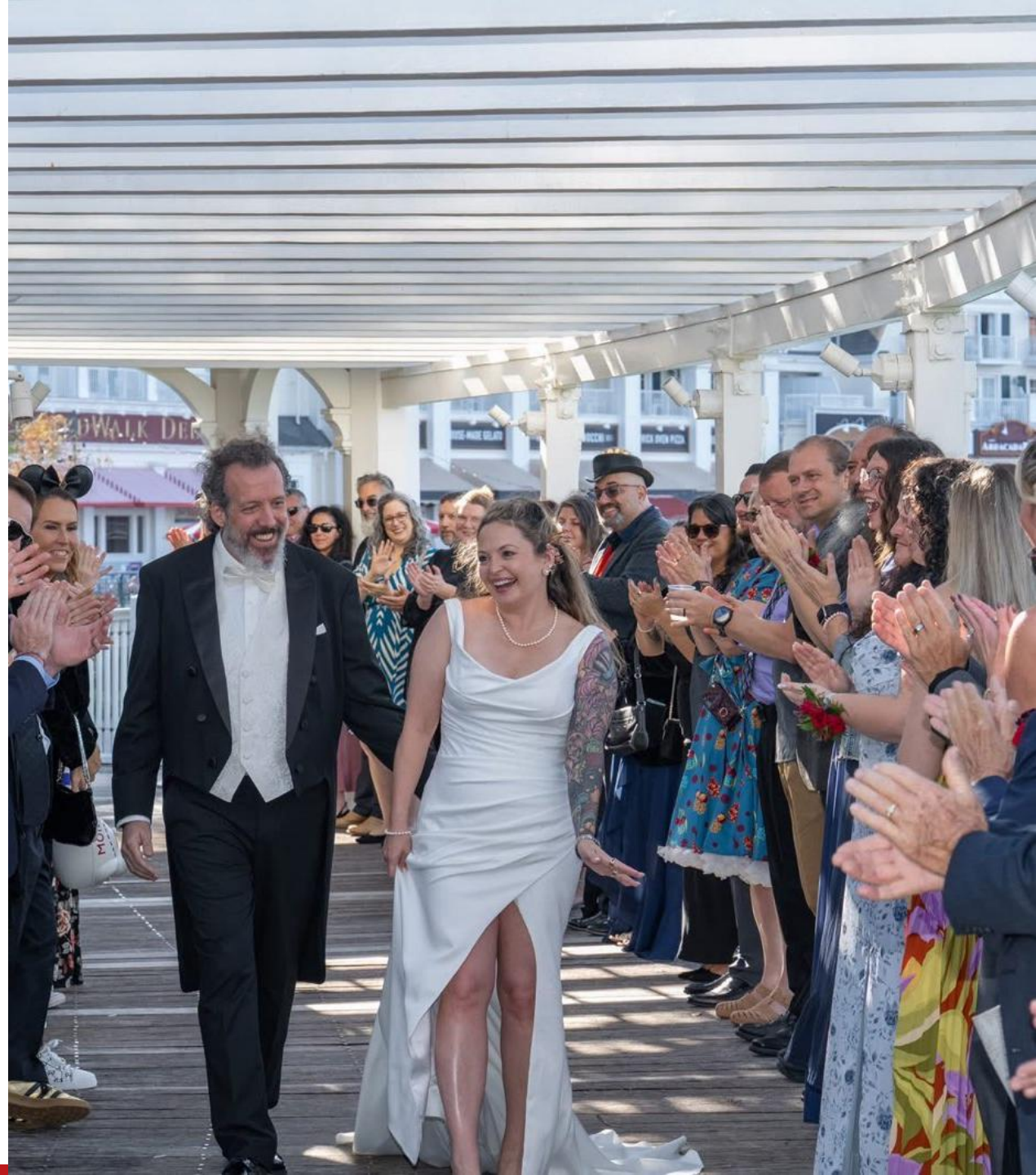
Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®

Kevin Tackett

- CEO - Secure Ideas, LLC
  - Founded in 2010
- IANS Faculty member
  - Since 2011
- Open-Source Fanatic
  - OWASP Leader
  - Former OWASP Global Board
  - Project Builder and Founder
- Speaker, Course Instructor, Author
  - Since 1991
  - SANS, ISC2, OWASP, DEF CON, Blackhat, etc.

- Other Interests
  - Warhammer (40K and AoS)
  - Woodworking
  - Husband and Father



Copyright © 2026 Secure Ideas LLC



We stopped building applications.
We started assembling them.

No one kept the manifest.

Copyright © 2026 Secure Ideas LLC

I. THE SITE MAP IS A LIE

The diagram is not production

WHAT THE DIAGRAM SAYS

- One clean data flow, start to finish
- A defined trust boundary at the edge
- One owner per system, clearly named
- Integrations that were reviewed once, at launch

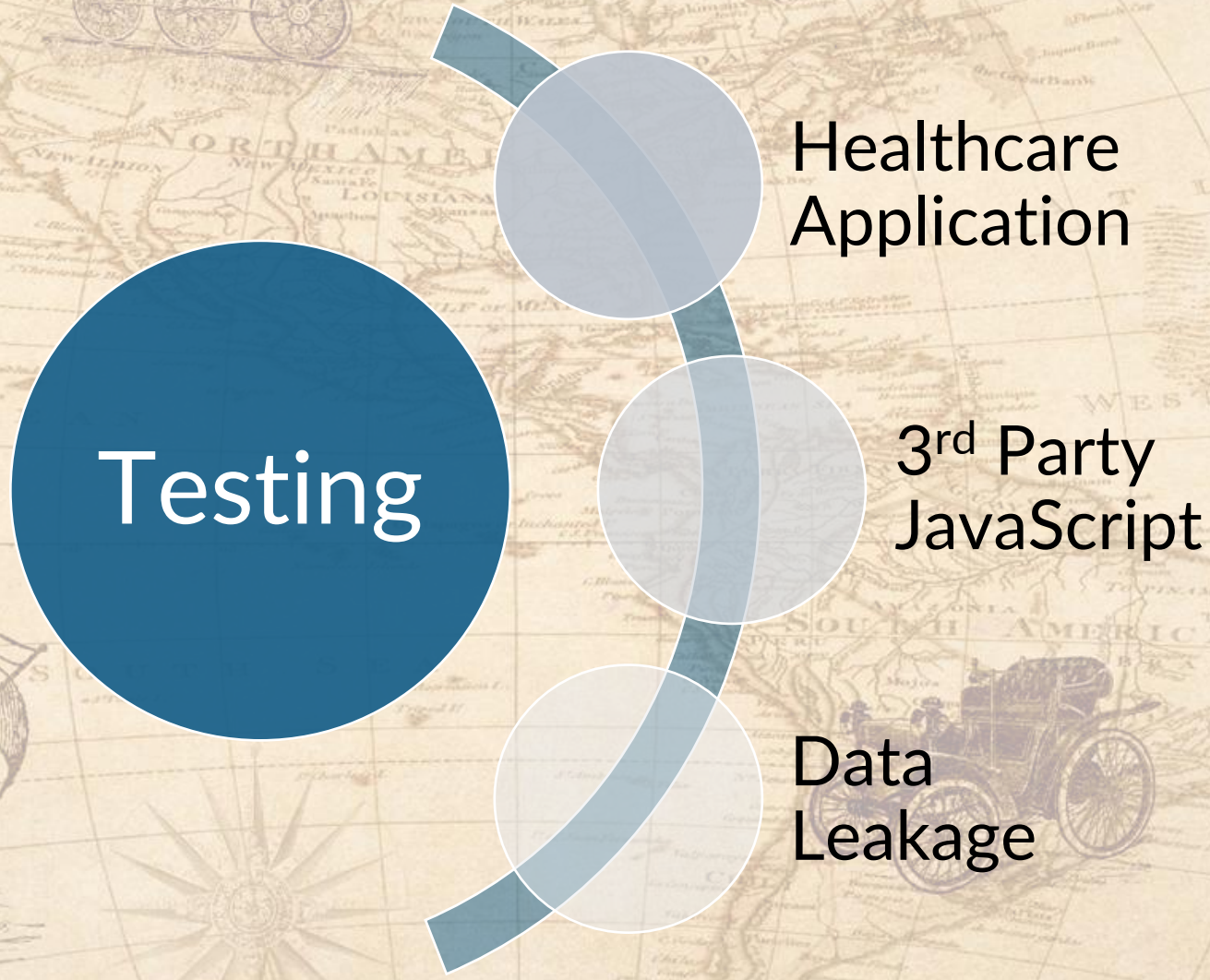
WHAT THE ENGAGEMENT FOUND

- Forgotten endpoints still wired to production data
- Trust boundaries assumed, never enforced
- Vendor systems nobody remembers
- An AI feature nobody scoped, added last quarter

Copyright © 2026 Secure Ideas LLC

I. THE SITE MAP IS A LIE

The Engagement



Copyright © 2026 Secure Ideas LLC

II. PASSAGES NOT ON THE BLUEPRINT

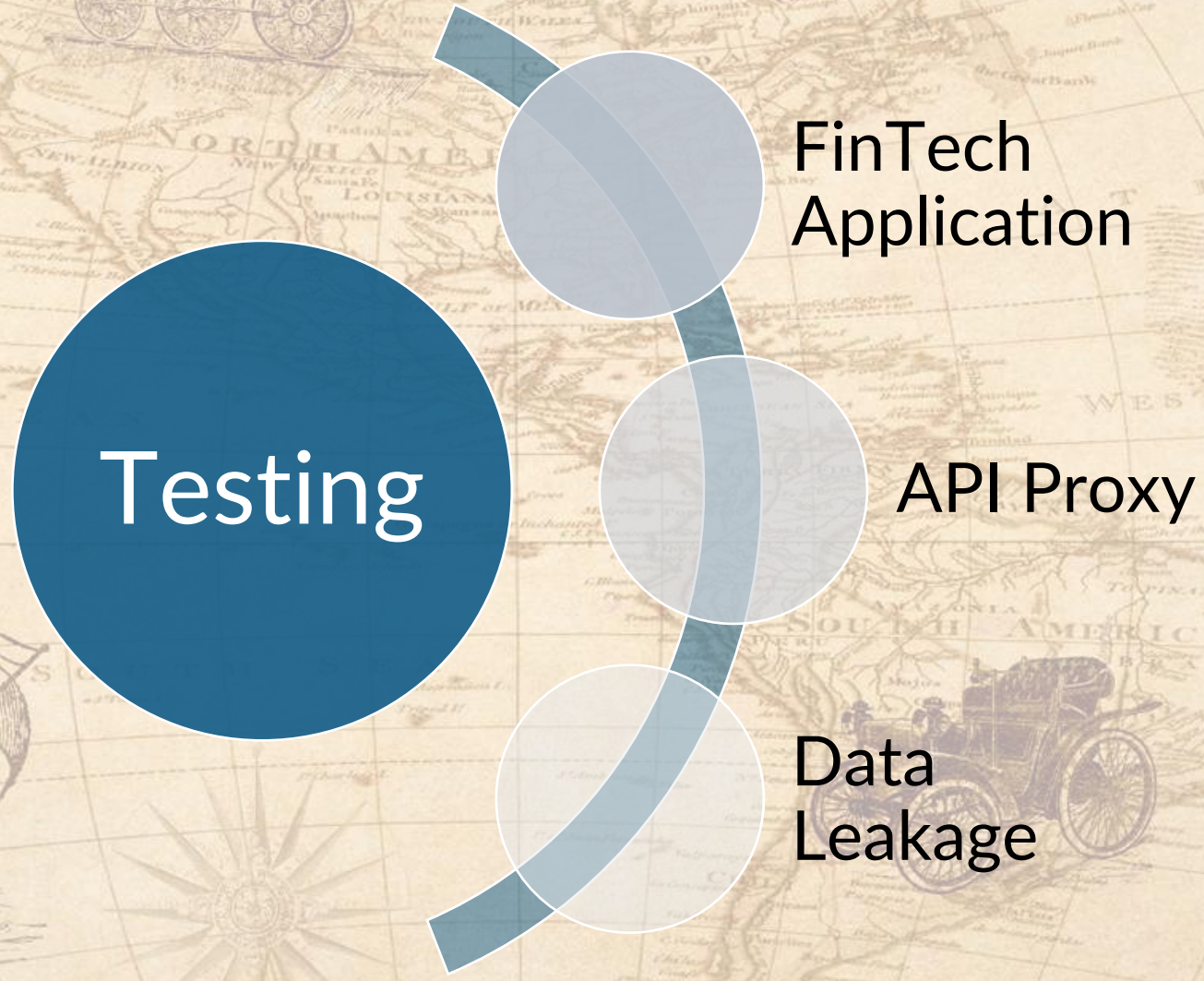
Production APIs quietly calling internal or dev-tier endpoints

- Internal and development-tier endpoints
  - Not supposed to be exposed
- Reachable anyway
  - Through a production API
- Internal is an overloaded term
  - And often misunderstood risk

Copyright © 2026 Secure Ideas LLC

II. PASSAGES NOT ON THE BLUEPRINT

The Engagement



Copyright © 2026 Secure Ideas LLC



Pieces are added by many people

Often with out speaking to each other.

Copyright © 2026 Secure Ideas LLC

III. IT HAD TO BE SNAKES

Libraries, APIs, and Authorizations

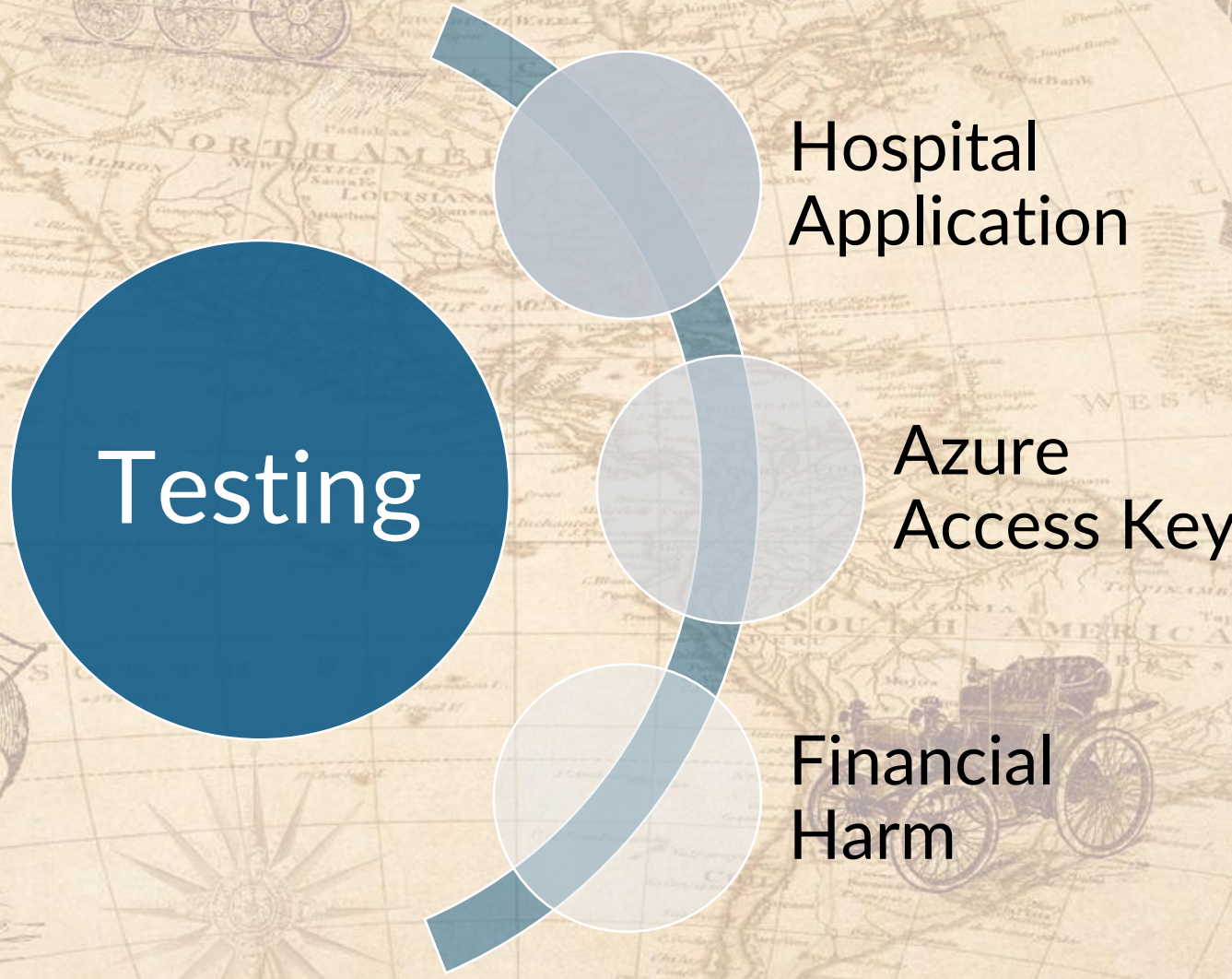
- Access to the systems
  - Yours and other company's
- How do we manage this access
  - Client-side, server-side, no idea?
- How do we test for this
  - Can we evaluate or actually attack?

Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®

III. IT HAD TO BE SNAKES

The Engagement



Copyright © 2026 Secure Ideas LLC



An assembled system inherits trust from every hand that ever touched it.



Copyright © 2026 Secure Ideas LLC

IV. SOMEBODY SWAPPED THE IDOL

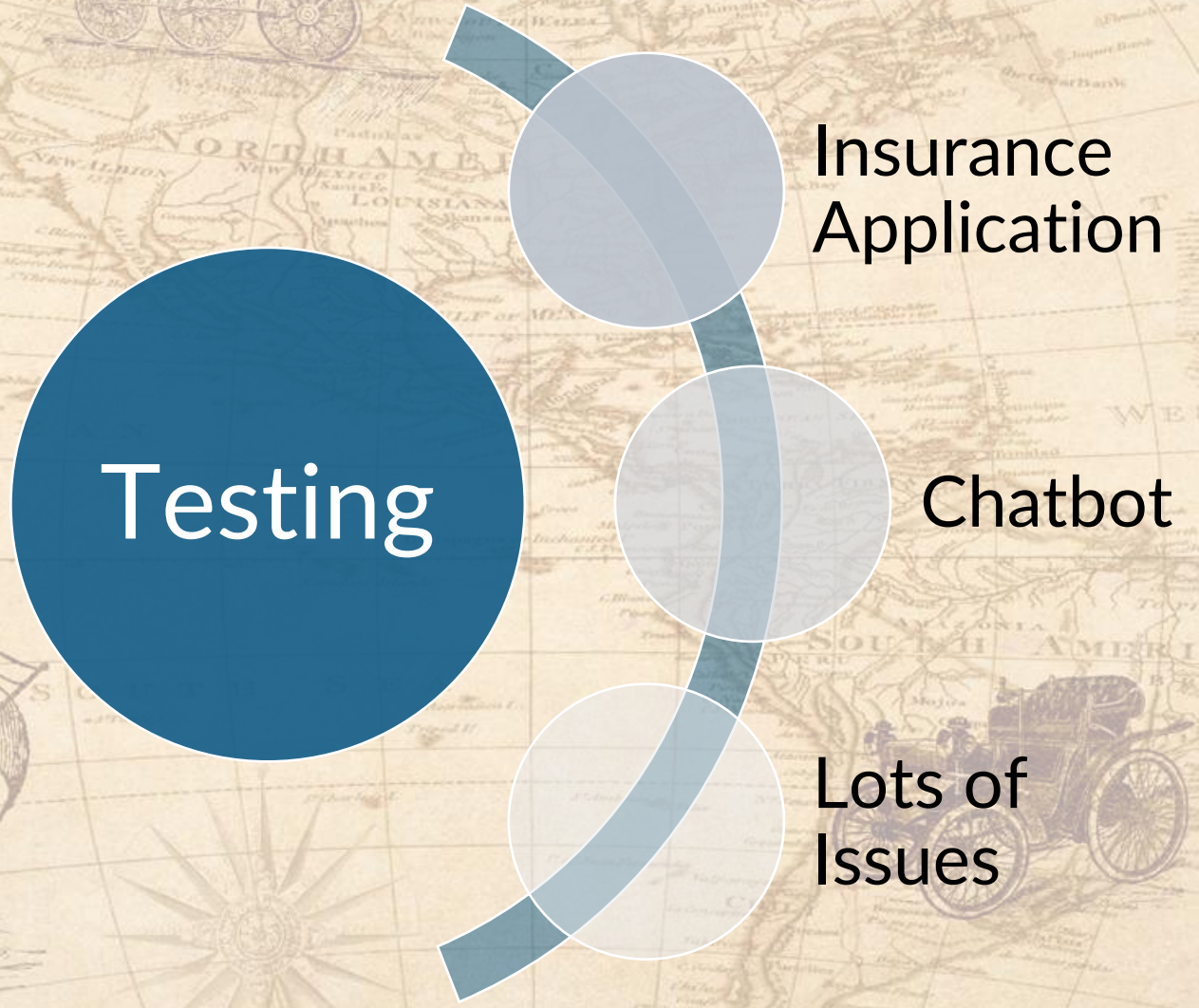
AI bolted onto systems never re-architected for it

- Chatbots
- Integrated Functions
- Third-Party Systems

Copyright © 2026 Secure Ideas LLC

IV. SOMEBODY SWAPPED THE IDOL

The Engagement



Copyright © 2026 Secure Ideas LLC



The newest assembled part nobody thought about guard rails

Copyright © 2026 Secure Ideas LLC

V. WHAT THE RUINS STILL TELL YOU

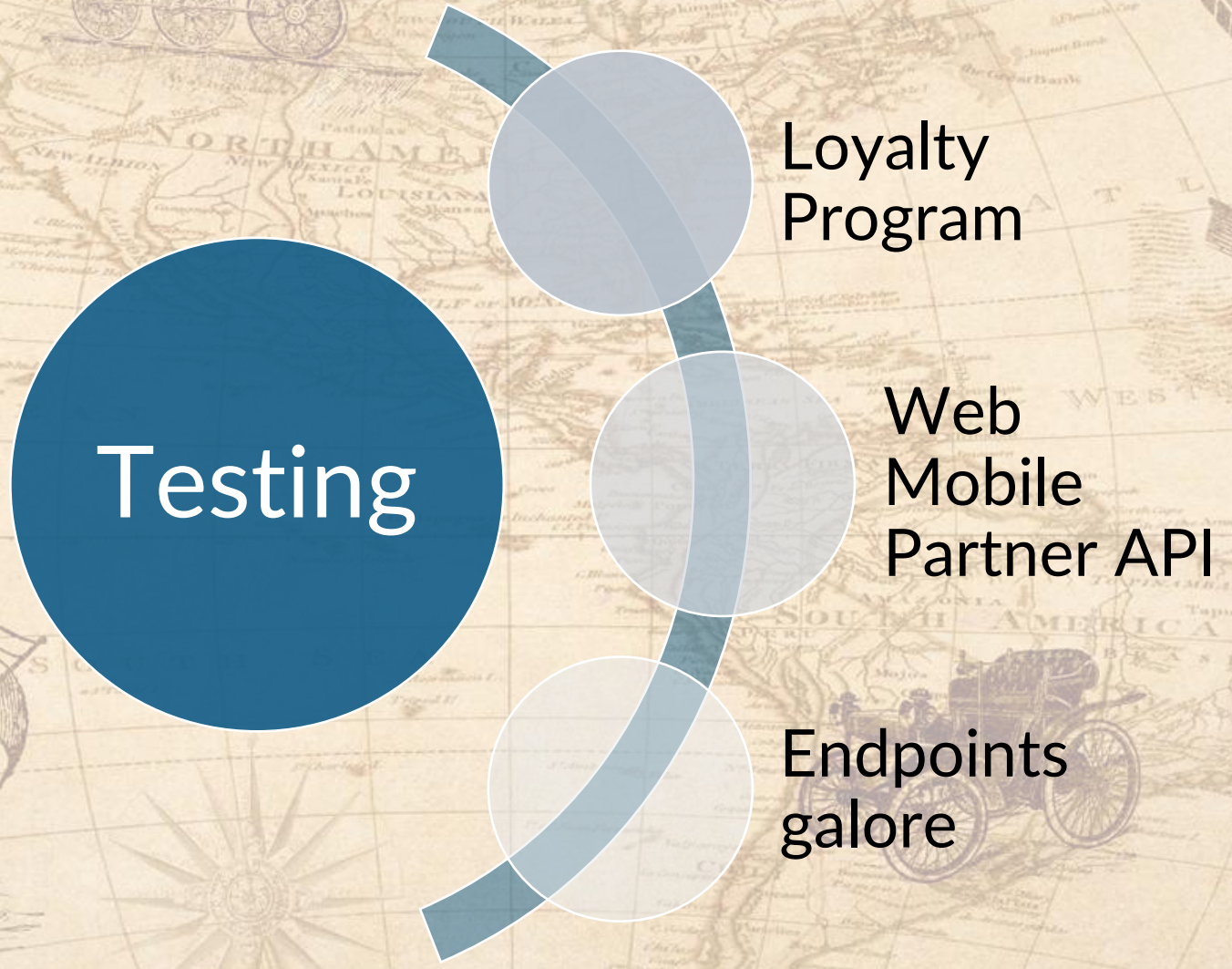
Where the seams exist

- Client-side JS
  - Routes and endpoints the UI skips
- Subdomain and DNS history
  - Often still reachable
- Certificate transparency logs
  - Exposes LOTS of targets (Beware White labeling!)
- Cloud metadata endpoints
  - Can we see infrastructure

Copyright © 2026 Secure Ideas LLC

V. WHAT THE RUINS STILL TELL YOU

The Engagement



Copyright © 2026 Secure Ideas LLC



Assembled things always leave seams
That we need to assess.

Copyright © 2026 Secure Ideas LLC

VI. NOT EVERY PASSAGE LEADS TO FORTUNE

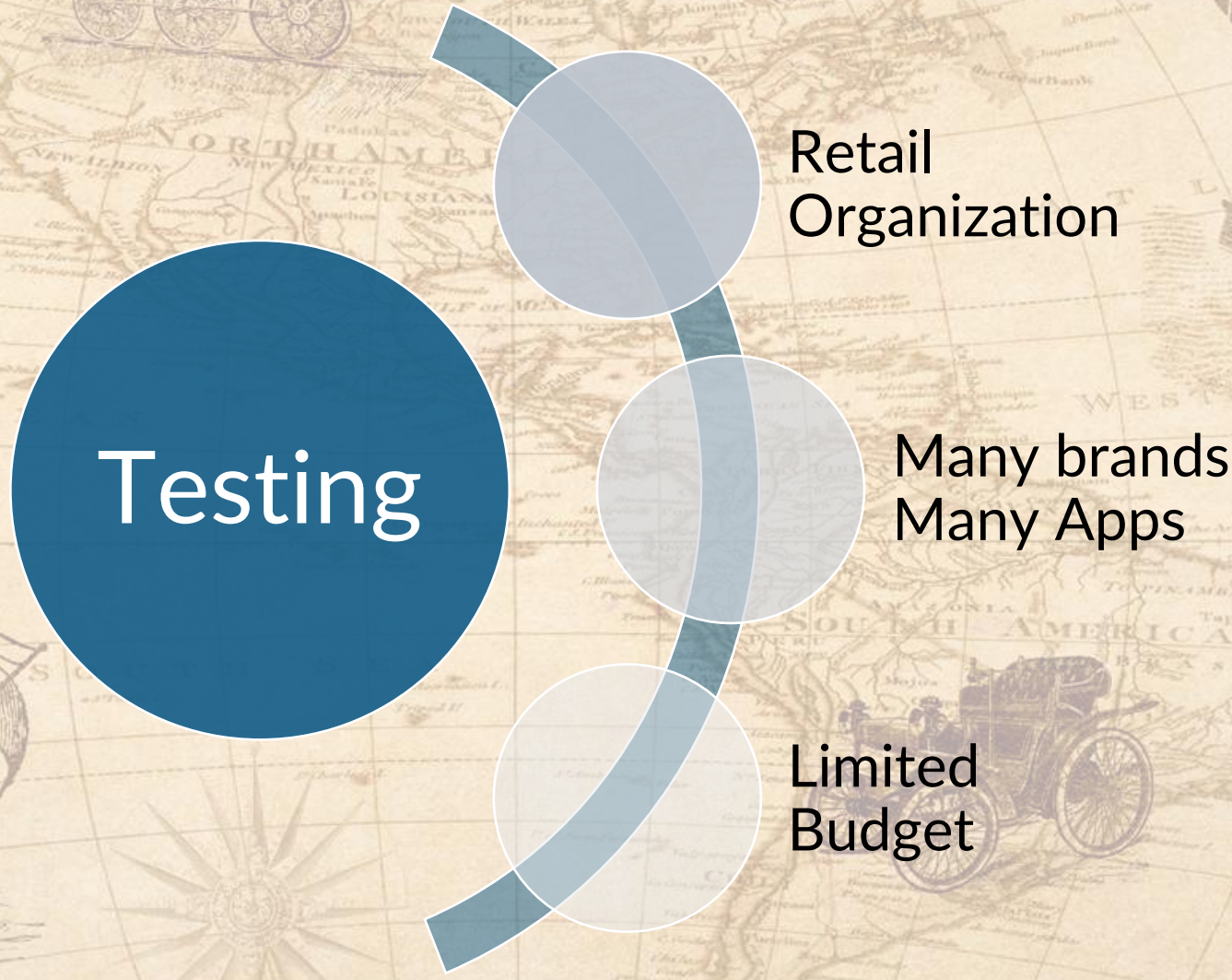
Triage: not everything uncovered deserves the same depth

- Every engagement surfaces more territory than the clock allows you to excavate fully
- Depth is a decision, not a default — and it has to be made on purpose, not by running out of time

Copyright © 2026 Secure Ideas LLC

VI. NOT EVERY PASSAGE LEADS TO FORTUNE

The Engagement



Copyright © 2026 Secure Ideas LLC



Say the depth decision out loud

Planning ahead for the testing.

Copyright © 2026 Secure Ideas LLC

Questions?



Kevin Tackett
kevin@secureideas.com
904-403-8024