

Ship of Theseus as a Service

Security Testing When Nothing is Truly Yours

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

Copyright © 2026 Secure Ideas LLC

Agenda



- Introductions
- Assembled Application
- Testing the Waters
- Shipping In Practice
- Testing the Waters
- Telegraphing the Results

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
  - Project Builder and Founder
- Speaker, Course Instructor, Author
  - Since 1991
  - SANS, ISC2, OWASP, DEF CON, Blackhat, etc.
- Board Member
  - BSidesJax
  - President

- Other Interests
  - Woodworking
  - Business and Team
  - Father



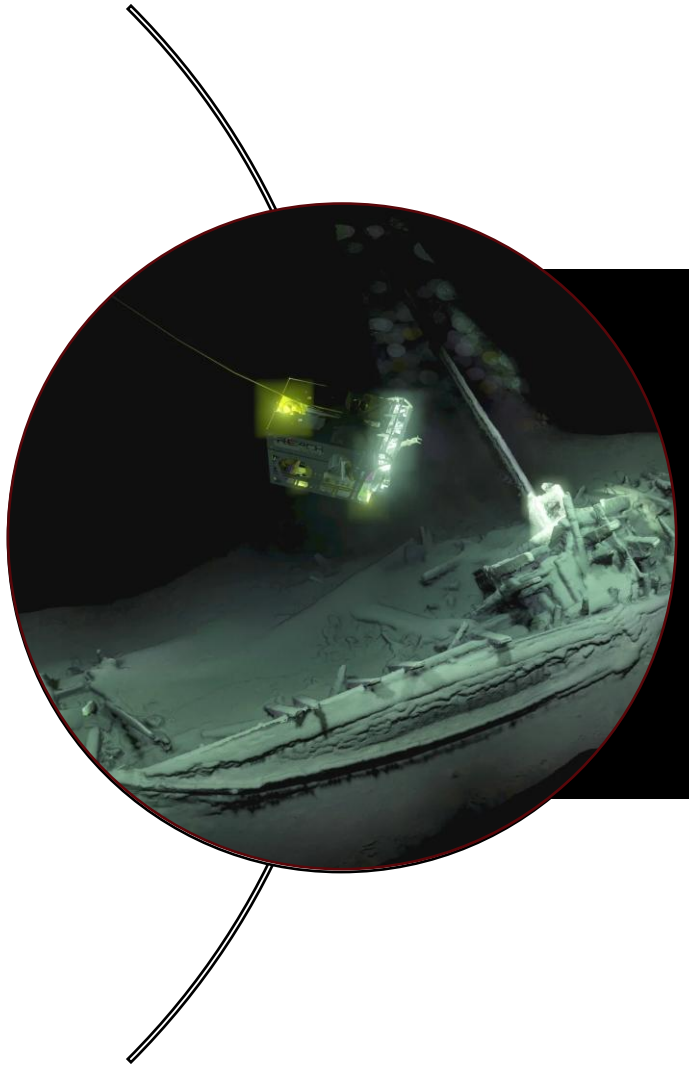
Copyright © 2026 Secure Ideas LLC

Introductions



Copyright © 2026 Secure Ideas LLC

Theseus's Hypothetical



Replacing Every Plank

Copyright © 2026 Secure Ideas LLC

Modern Reality

Development

- Assembled
  - More Often than Not
- Third-Party Systems
  - Libraries
  - APIs
- AI
  - Yes, we need to discuss it
  - No, it really isn't that different

Testing

- SAST
  - Your parts
- DAST
  - Vulnerability Assessments
  - Limiting
- Penetration Testing
  - Deep dive
  - Human Run

Copyright © 2026 Secure Ideas LLC
Secure Ideas professionally evil®

Assembled Applications



Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®

Building the Ship

- Modern Application Ingredients
  - Fronted frameworks
  - CDN-hosted Libraries
  - Various Processors and APIS
  - AI and ML services
  - Cloud Systems
  - Analytics and Marketing platforms
  - Your Code!



Copyright © 2026 Secure Ideas LLC

Trust Relationships

- Every external component introduces a trust relationship
  - Authentication and SSO
  - AI Service leakage or guardrails
  - CDNs are just assumed to be good

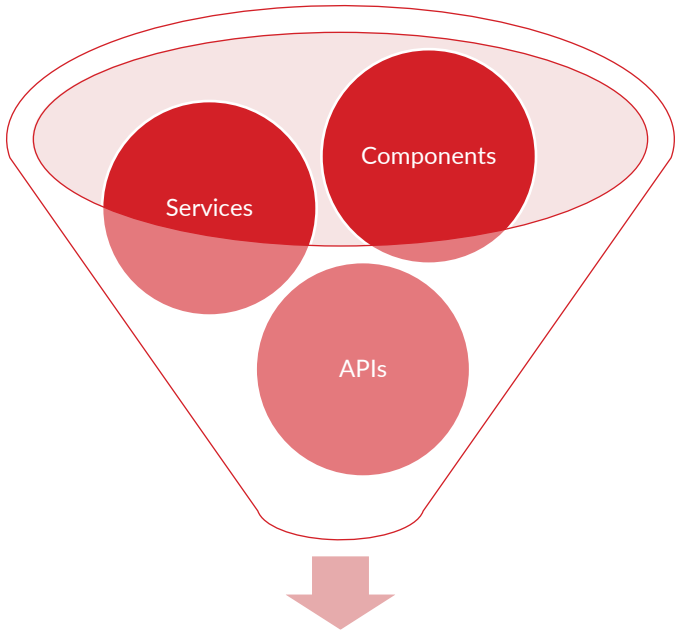
- Trust often fails to assumptions
  - Test these!



Copyright © 2026 Secure Ideas LLC



Ownership Inventory



Application Ownership

Copyright © 2026 Secure Ideas LLC

Testing the waters



Copyright © 2026 Secure Ideas LLC

Archeology in Practice



Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®



Scoping Issues

- Traditional testing assumes Ownership
  - Even then it is often wrong
- What are the boundaries?
  - Who controls what
  - Who sees what
- Rules of Engagement
  - More difficult to ensure compliance

Access Issues

- Not just a “can I access this” issue
  - Reachability is often fine
  - Third-parties are on the Internet
- Test Instance Issues
  - Testing in non-prod
  - Data retention and usage
  - Transaction reversal
- Compliance Issues
  - Contractual limitations
  - Notification limitations



Copyright © 2026 Secure Ideas LLC

Visibility Issues

- Web interfaces are easy
  - We want to believe
- What about APIs and AI services
  - Data often goes into a blackhole
    - At least to our tester's perspective
- Relates strongly to the access issues



Copyright © 2026 Secure Ideas LLC



Responsibility Issues

- Who is responsible
  - For the fixes
  - For the issues
  - For the understanding
- Shared responsibility models are assumed to answer this
  - Basically, makes no one test.

SecureIdeas
professionally evil®

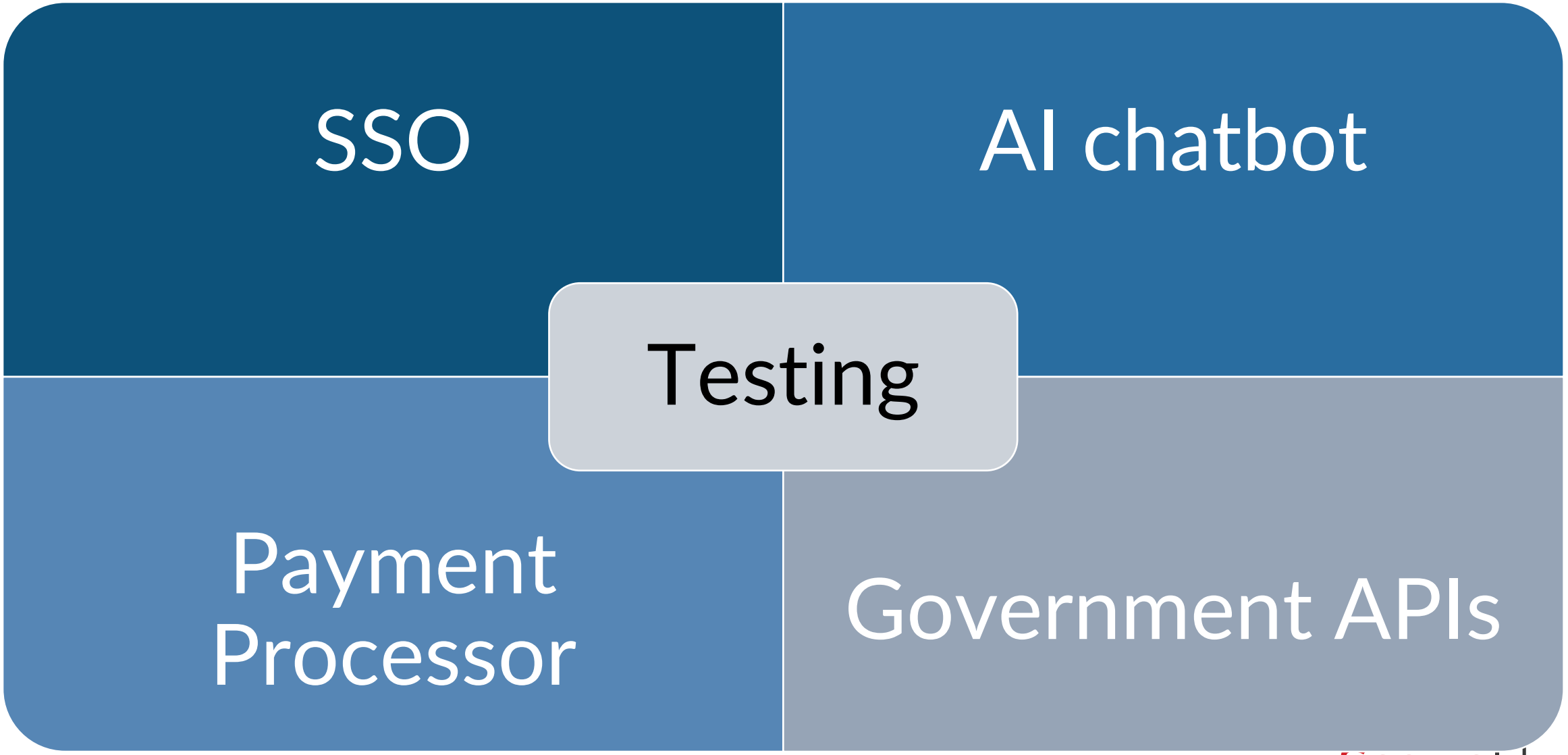
Shipping in Practice



Copyright © 2026 Secure Ideas LLC

Secure Ideas
professionally evil®

Practical Examples



Copyright © 2026 Secure Ideas LLC

Testing the Waters

You may not own the ship, but you own the seams



Copyright © 2026 Secure Ideas LLC



Scoping Steps

- Discovery
  - Map dependencies
  - Identify APIs and Integrations
- Dependency Mapping
  - Understand ownership
  - Verify transactions and feature usage
- Risk-Based Prioritization
  - Data sensitivity
  - Access levels
  - Blast radius

Secure Ideas
professionally evil®

Focusing



Integration Points

Data Flows

Trust Boundaries

Failure Handling

Transaction Functions



Copyright © 2026 Secure Ideas LLC

Telegraphing the Results



Copyright © 2026 Secure Ideas LLC

Certificates of Authenticity

- What happens with discovered issues?
  - Who do we tell
  - Can we publicize it
- Understanding beyond the flaw
  - Who owns the fix
  - Who drives the remediation



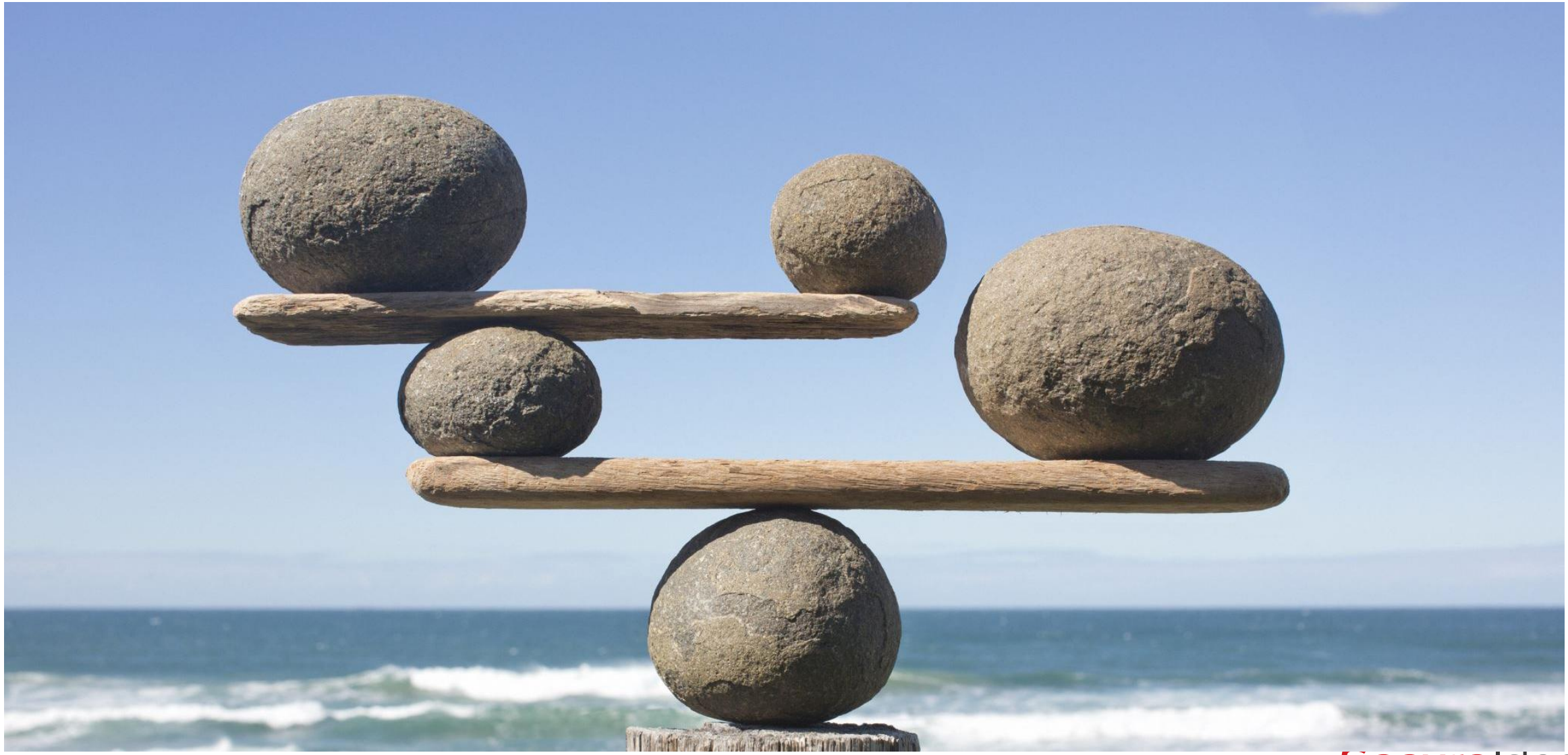
Copyright © 2026 Secure Ideas LLC

Risking the Waters



Copyright © 2026 Secure Ideas LLC

Exhibiting the Artifacts



Copyright © 2026 Secure Ideas LLC

Questions?



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