Scapien Synergy Program

Turning validated risk into real outcomes — together

The problem partners run into

Most security engagements don't fail at finding issues. They fail at turning those issues into action.

A customer receives a report. Different teams interpret the findings in different ways. Security pushes urgency, IT questions feasibility, and leadership asks for justification. What should have been a straightforward next step turns into a prolonged and inefficient cross functional discussion.

From a partner's perspective, this creates a familiar set of challenges:

- You are brought in to help identify or fix problems, but not always involved in deciding how things are prioritized.
- Time is spent explaining and re-explaining findings instead of moving to delivery
- Scope becomes fragmented, delayed, or reduced before meaningful work begins

Over time, this affects both execution and revenue. Work is harder to define, harder to approve, and harder to sustain.

What Scapien changes

Scapien shifts the conversation from "here are the issues" to "here is what can actually happen, what it means, and what needs to be done next."

Instead of relying on severity labels or tool output, Scapien shows how an issue behaves in practice — how an attacker could move, what they could reach, and what the consequences would be.

That clarity removes the need for interpretation.

The discussion moves quickly from uncertainty to action:

- The risk is understood in concrete terms
- The business impact is visible
- The next step becomes obvious

At that point, the conversation is no longer about whether something matters. It is about how to address it.

Who does what

Scapien proves what is exploitable, defines business impact, provides prescriptive remediation guidance, and verifies that fixes hold over time.

Partners bring environment expertise, lead remediation execution, design architecture improvements, and provide ongoing advisory support.

There is no overlap in delivery. Scapien defines and validates the problem. You design and implement the solution. The customer gets clarity, justification, and desired business outcomes.

How this translates into partner value

When the problem is clearly understood, three things improve immediately: prioritization, decision speed, and the ability to define meaningful work.

Prioritization becomes cleaner

Instead of working through a long list of competing findings, the customer is looking at a smaller number of issues tied to real impact. This allows you to focus effort where it matters and avoid low-value or unnecessary work.

Decisions happen faster

When the impact is clear, internal alignment becomes easier. Security, IT, and leadership are no longer debating abstract severity — they are reacting to something concrete. This reduces delays and makes approvals more straightforward.

Work is easier to scope and deliver

Because the issue is clearly defined, the remediation work becomes clearer as well. Engagements start with better structure, fewer revisions, and stronger alignment between expectation and execution.

In practical terms, this means:

- Less time spent selling the problem
- More time spent delivering the solution
- Engagements that are larger, cleaner, and easier to execute

Becoming part of the decision process

One of the most important shifts is where you sit in the customer relationship.

When risk is unclear, decisions are made internally, and partners are brought in afterward. When risk is clear and tied to impact, customers need help executing.

Conversations become more strategic and less about fulfillment.

You are no longer only responding to defined work. You are helping define:

- What gets prioritized
- What gets funded
- What gets executed

Partner Revenue Snapshot

Partners working with Scapien engagements report:

- Remediation engagements that are faster to scope because the problem & fix are already defined
- A clear path from one validated finding to billable design, implementation, and verification work
- Ongoing validation program creates follow-on engagements instead of one-off projects
- Customers that act faster on remediation because the business impact is visible from the start

“You show them the risk and tell them what the business impact is and how to fix it. That makes it so much easier for us to justify getting budget.”

— Scapien Synergy Partner

What the engagement economics look like

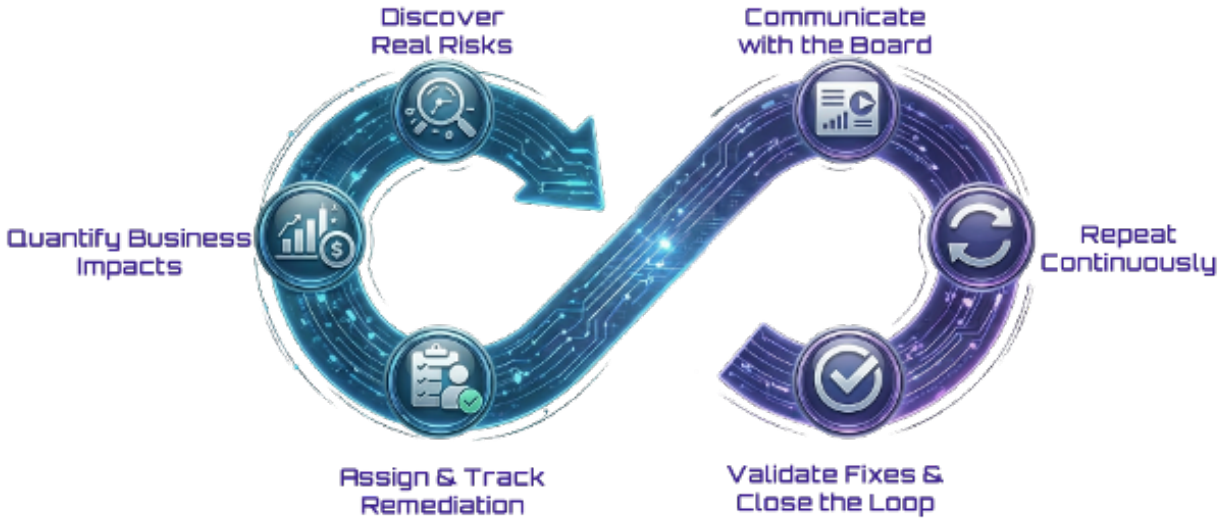
A single validated finding typically generates a remediation engagement involving design, implementation, and verification. That work is clearly scoped, defensible to the customer’s leadership, and naturally extends into ongoing validation.

Consider what a typical engagement produces:

- The initial validated finding defines a clear scope of work with measurable outcomes
- Remediation execution — segmentation redesign, access control hardening, IAM restructuring — becomes billable work that the customer has already agreed matters
- Verification confirms the fix worked, creating a documented outcome the customer can show their board or auditors
- As environments change, continuous validation surfaces new priorities — each one a potential new engagement

This is not a single-invoice relationship. Each cycle of validation, remediation, and verification creates a natural reason to stay engaged and a defensible basis for the next scope of work.

The coordination itself — managing remediation workflows, tracking progress, aligning teams around priorities — becomes a service partners can deliver alongside execution. That is additional value the customer needs and is willing to pay for.



Practical examples

Example 1: Lateral movement — from proof to remediation to closure

What was proven:

Lateral movement from an application server to a domain controller via a misconfigured service account.

Why it mattered:

Potential for full domain compromise and access to critical systems.

What changed:

- Network segmentation redesigned (3 → 60+ segments)
- Privileged access controls strengthened
- Attack path verified closed through retesting

Partner role:

Designed and implemented segmentation and access control improvements, and supported validation.

Example 2: Cloud privilege escalation — from exposure to governance

What was proven:

Over-permissioned IAM role allowed escalation to administrative access.

Why it mattered:

Exposure of sensitive data and control of production systems.

What changed:

- IAM policies restructured to least-privilege
- Access boundaries enforced
- Continuous validation ensures escalation paths remain closed

Partner role:

Led IAM redesign, governance implementation, and policy standardization.

Each example started with a single validated finding and became a broader engagement involving design, implementation, and ongoing verification. Two different types of work. Two different revenue streams. Both clearly scoped from the start.

Outcomes — for customers and for partners

For customers, the outcome is clarity and confidence. They understand what matters, they fix it faster, and they can see that it is actually resolved.

For partners, the focus is on business outcomes and strategic direction. You are better positioned to guide decisions, define work, and stay engaged over time.

In both cases, the result is the same: security work becomes more focused, more measurable, and more aligned with real business impact.

Let's talk

Contact Scapien at info@Scapien.com to discuss whether our validation-led security model fits your delivery approach. In 15 minutes, we'll walk through a real engagement, the economics, and the next step.