



The Mobilization Gap:

Why Your Security Program Needs a System of Action

Or Naim | VP Product Management
Reclaim Security

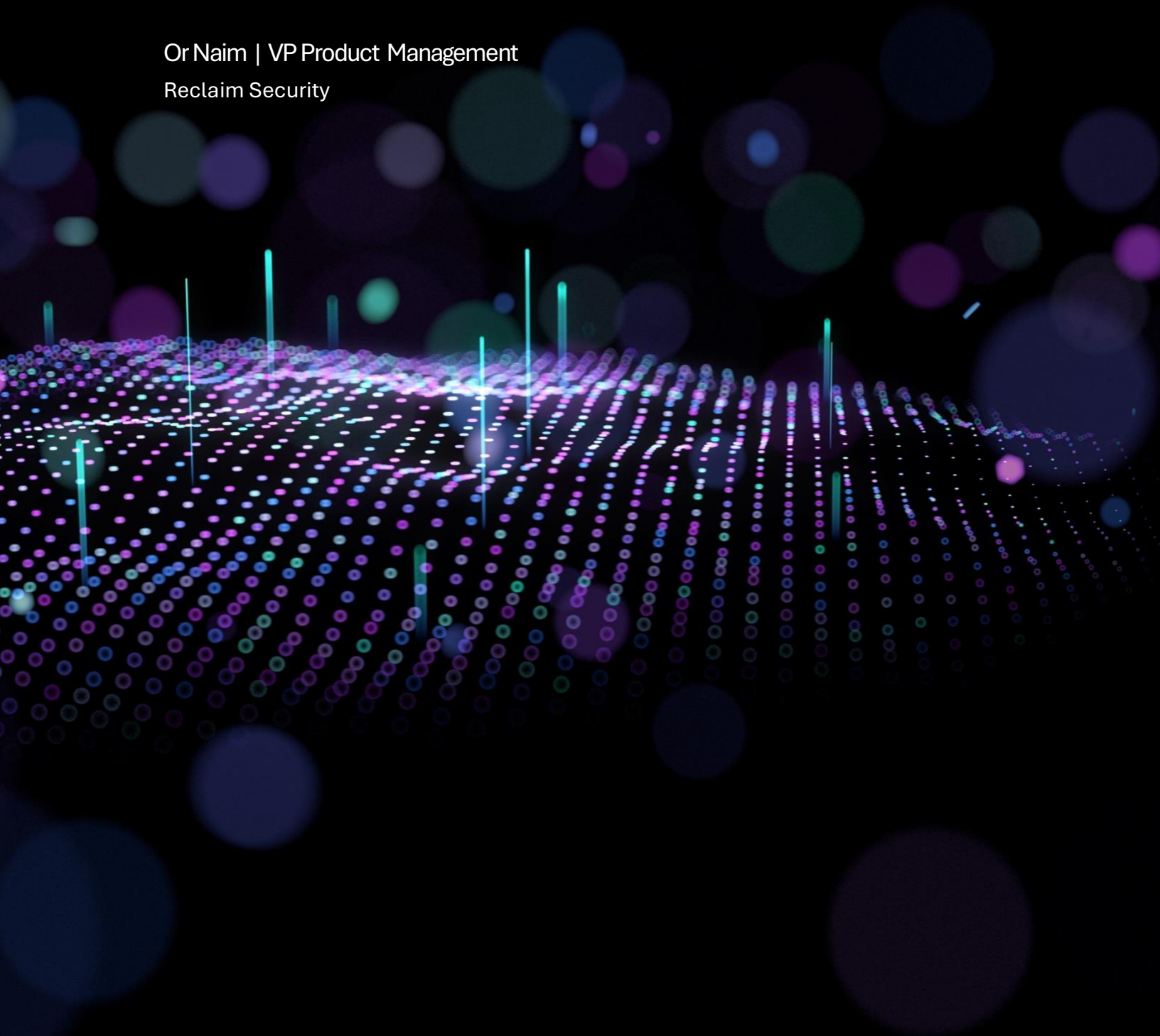




Table of Contents

1. The System of Record: The Trap of "Better Visibility"	3
2. The Automation Paradox: When Prioritization Isn't the Bottleneck	3
3. The Missing Link: The Three Pillars of Mobilization	3
4. The "Super Engineer" Profile	4
5. Scaling the Future: AI as the System of Action	5
Conclusion: Focus on the Outcome	5

For over a decade, I have worked with global enterprises to proactively remediate critical exposures before adversaries can take advantage of them. During this time, I've seen organizations invest millions in the latest security stacks, only to find their actual risk posture remains stagnant.

After ten years in the trenches, I have arrived at a fundamental conclusion:

Knowing what to fix and knowing how to get it done are two entirely different disciplines.

Knowing what needs to be done and knowing how to get it done are two entirely different skill sets.


To understand why so many mature security programs stall, we have to look at the distinction between the **System of Record** and the **System of Action**.

Before we jump in, I want to highlight Jonathan Nunez from Gartner for leading the charge in this area. He's been an influential voice pushing for this outcome, and I'm glad to see we are in complete alignment.

Closing the Mobilization Gap: Moving From Visibility to Action


The Problem: The Mobilization Gap

Visibility is not Risk Reduction.




Knowing what to fix and knowing how to get it done are two entirely different disciplines.

Prioritization is Rarely the Bottleneck.




The real bottleneck is mobilization—getting human teams to change production environments.




3x Less Likely to Suffer a Major Breach

Mature exposure management programs are projected to reach this goal by 2026.


The Solution: The 3 Pillars of Action



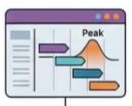
Simulation: Knowing the Implications
Validating that patches won't disrupt production to move from "hoping it works" to "knowing it works."



Translation: Speaking Operational Language
Converting technical CVEs into business impact statements regarding uptime, revenue, and compliance.



Planning: Aligning Security with Reality
Transforming business context (like peak sales periods) into tactical, phased rollout plans.



	System of Record (Passive)	System of Action (Active)
Primary Goal	Visibility and Insights	Remediation and Outcome
Focus	Aggregating & Prioritizing Data	Simulation, Translation, & Planning
Output	A "More Accurate" List of Problems	An "Effective Path" to a Solution



1. The System of Record: The Trap of "Better Visibility"

In the world of exposure management, most "Security Tools" are, in reality, Systems of Record. A System of Record is designed to solve data-related problems. Its primary goal is visibility and insights. It helps you aggregate data from multiple sources, understand the "current state" of your environment, and track the lifecycle of a vulnerability for auditors.

While these are essential, they are passive. They help you better understand the situation, and the best ones help you make a decision. But they don't move anything.

Many organizations have recently matured their operations into **Continuous Threat Exposure Management (CTEM)**. They have successfully moved from reactive vulnerability management to a proactive operation that takes into account threat and business context.

Yet, too many programs still fail to impact the bottom line. They have defined the target perfectly, but they haven't delivered the outcome. They have built the ultimate System of Record, but they lack the vehicle to reach the destination.

(Quick real-world note: Industry reports show that organizations with mature CTEM programs are projected to be up to 3x less likely to suffer a major breach by 2026—yet many still struggle to reduce risk because mobilization remains largely manual.)

2. The Automation Paradox: When Prioritization Isn't the Bottleneck

To solve the lack of impact, the industry's knee-jerk reaction was to introduce automation. We automated the prioritization logic, which significantly increased our "prioritization capacity." We can now sort through a million vulnerabilities faster than ever.

However, organizations are quickly realizing that prioritization is rarely the actual bottleneck. The real bottleneck is **Mobilization**—the act of getting a human in a different department (IT, DevOps, Cloud Ops) to change something in a production environment.

When you automate the "finding" part of the process, you often just create a larger pile of high-priority work that the IT team doesn't have the capacity or the context to execute. Automation creates excess capacity in the System of Record, but without a System of Action, that capacity turns into friction and idle FTEs.

3. The Missing Link: The Three Pillars of Mobilization

Years ago, the industry introduced a new persona: the "Vulnerability Manager." But as the gap between finding and fixing widened, that role became too administrative.

To bridge the gap today, we need a new hybrid persona: **Exposure Mobilizer** - The Mobilization Problem Solver.



This role serves as the engine of the System of Action. They don't just "report" on risk; they operationalize it through three critical functions:

I. Simulation: Knowing the Implications The number one reason IT teams push back on security requests is the fear of "breaking the business." The Mobilizer uses simulation to answer the question: "What happens if we actually do this?"

- They validate that a patch or configuration change won't disrupt production.
- They provide the evidence needed to lower the perceived risk of remediation.
- **Goal:** Moving from "we hope it works" to "we know the impact."

II. Translation: Security Findings into Operational Language Security speaks in CVEs and exploitability. IT speaks in uptime and maintenance windows. Business speaks in revenue and compliance.

- The Mobilizer translates a technical finding into operational language.
- Instead of saying "CVE-2024-XXXX is critical," they say, "This database configuration allows unauthorized access to customer data; we need to update this specific library to prevent a breach while maintaining 99.9% uptime."
- **Goal:** Creating shared understanding and urgency across silos.

III. Planning: Transforming Business Context into Rollouts Prioritization tells you what is important; Planning tells you how it gets done.

- The Mobilizer takes business context (e.g., "Don't touch the retail servers during Black Friday") and transforms it into a tactical rollout plan.
- They coordinate across business units, ensuring that remediation happens in a phased approach that respects the organization's operational reality.
- **Goal:** Aligning security urgency with business continuity.

4. The "Super Engineer" Profile

This Mobilization Problem Solver is a "**Super Engineer**" sitting at the intersection of three domains:

- **Security Domain Expertise:** Threat, exposure, and technical knowledge of Endpoint, Network, and IAM.
- **Program Management Skills:** The ability to navigate corporate politics and drive complex projects across departments.
- **IT Experience:** The empathy and technical knowledge to understand why a "simple patch" is never actually simple.



5. Scaling the Future: AI as the System of Action

The reality is that most organizations—unless they are in the Fortune 100—cannot afford to staff a team of dedicated Mobilization Problem Solvers. It is a roles-rich, expensive endeavor.

This is where the industry is heading: **AI agents will fill the mobilization gap.**

The next evolution of exposure management isn't a better scanner; it's an **AI-driven System of Action**. Imagine AI agents that work with a "human-in-the-loop" to:

1. **Simulate:** Automatically gather the evidence IT needs to feel safe about a change.
2. **Translate:** Draft technical instructions and business justifications tailored for specific owners.
3. **Plan & Coordinate:** Handle the back-and-forth scheduling and validation, closing the loop without manual ticket updates.

This is critical for the Global 2000 and the mid-market. It moves the focus away from SOC-related automation (reactive) and toward **Preemptive Coordination** (proactive).

Conclusion: Focus on the Outcome

If your security program is feeling "stuck," it is likely because you are over-indexed on your System of Record and under-indexed on your System of Action.

- CTEM defines the target, but doesn't deliver the outcome. Visibility alone is not risk reduction.
- Automation creates idle capacity unless it is redeployed toward the "last mile" of fixing.
- Simulation, Translation, and Planning are the functional gears that turn a finding into a fix.

We must stop treating security as a data problem and start treating it as a process problem. The goal isn't to have the most accurate list of problems—it's to have the most effective path to the solution.

Quick self-audit for leaders: Review your program metrics. What percentage of your top-prioritized exposures are actually remediated within SLA? If that number isn't climbing despite better visibility and automation, it's time to invest in mobilization—whether through hybrid "super engineers" today or AI agents tomorrow.