ARBITIUM

ARBITIUM INSIGHTS

Why We Started Arbitium

John Remo, Co-Founder & CEO | January 8, 2026

There's a moment every security operator knows. It's 2 AM. Your SIEM just lit up. Forty-seven alerts in twelve minutes. Your on-call analyst is already triaging something else. The playbook says escalate, but escalate to whom? The senior engineer quit last month. The one before her left six months ago.

You've got a $400K SOAR platform, a best-in-class EDR, and a threat intel feed that costs more than some people's houses. And right now, at 2 AM, none of it matters, because the work still needs a human being to do it.

I've lived that moment. Too many times.

The Promise That Never Delivered

Before starting Arbitium, I spent years running engineering and security operations for global enterprises. The kind of organizations where a breach isn't a news story. It's an existential event. Over that time, I sat through more vendor pitches than I can count. Every one of them had the same promise: This product will solve your problem.

And honestly? Many of them were good products. SIEM gave us visibility. SOAR gave us orchestration. EDR gave us endpoint coverage. Threat intel gave us context. Each tool made the team more informed, more efficient, a little bit faster.

But none of them solved the problem.

The problem isn't detection. We've actually gotten remarkably good at finding threats. CrowdStrike's 2025 Global Threat Report puts the average breakout time (how fast an attacker moves laterally) at 48 minutes. We can often detect that movement within minutes.

The problem is what happens next.

The Execution Gap

When a threat is detected, someone has to act. Someone has to investigate the alert, correlate it with other signals, determine if it's real, decide on the right response, execute that response across potentially dozens of systems, and verify it worked. That "someone" is a human being, usually an exhausted one.

The industry has a term for this: the cybersecurity talent shortage. Right now there are 4.8 million unfilled cybersecurity positions globally. But from where I sat as an operator, the framing always felt wrong. It wasn't that we couldn't find enough people. It was that we were asking people to do work that shouldn't require people at all.

Every time I added a new security tool, I needed to add headcount to operate it. More tools, more alerts, more analysts. The math never worked. You can't hire your way out of a problem that scales exponentially while your team scales linearly.

When AI Changed the Equation

For years, AI in cybersecurity meant better detection. Machine learning models that could spot anomalies. Natural language processing that could parse threat reports. It was analysis, impressive analysis, but still analysis. The output was always the same: Here's what we found. Now go do something about it.

Then something shifted. AI moved from analysis to action. Large language models could reason about complex, multi-step problems. Agentic architectures could plan and execute sequences of tasks autonomously. Suddenly, the gap between "we found a threat" and "we stopped a threat" didn't need a human in the middle.

That's when I knew it was time to build.

What Arbitium Is

Arbitium is an autonomous AI execution platform for cybersecurity. We connect to your existing security tools: your CrowdStrike, your Okta, your AWS, your Splunk, and we do the work that used to require your team.

When a threat is detected, Arbitium's AI agents reason across alerts and context, determine the right response, and execute precise API-level remediations directly in your environment. No playbooks. No ticket queues. No 2 AM phone calls.

We don't replace your security stack. We replace the manual labor that sits between your security stack and actual security.

Why Now

The timing isn't accidental. Three things converged to make this possible:

First, AI matured from analysis to execution. The reasoning capabilities of modern AI systems are now sophisticated enough to handle the nuanced decision-making that incident response requires.

Second, the threat landscape accelerated beyond human capacity. With 79% of attacks now malware-free and adversaries moving laterally in under an hour, there's simply no way manual response can keep pace.

Third, the economics broke. The average data breach now costs $4.44 million globally, and $10.22 million in the United States, an all-time high. Organizations are spending more on security than ever and getting less protection per dollar, because the bottleneck isn't their tools. It's the gap between those tools and action.

What's Next

We're building Arbitium for the operators, the people who've sat in the chair at 2 AM and felt the weight of knowing that the difference between a contained incident and a catastrophic breach is whether a human can move fast enough.

We believe that in five years, the idea of a human manually triaging alerts and executing incident response will feel as outdated as manually updating virus signatures. The technology exists to close the loop from detection to action autonomously. We're here to build it.

If you're headed to RSAC 2026 this March, come find us. We'd love to show you what autonomous execution actually looks like.

And if you're an operator who's lived that 2 AM moment, we built this for you.

John Remo is the Co-Founder and CEO of Arbitium. Before founding the company, he led engineering and security operations for global enterprises across multiple industries.

Sources referenced: CrowdStrike 2025 Global Threat Report; IBM Cost of a Data Breach Report 2025; Palo Alto Networks 2026 Cybersecurity Forecast.