

JOHN SABO

Mesa, AZ | john@johnsabo.org | LinkedIn: linkedin.com/in/realjohnsabo

Summary

Full-stack engineer and security automation architect. Six products built and shipped in 2026: a two-sided marketplace SaaS with Stripe subscriptions and a 2.76M-row database (Home Staked), a live agency SaaS with affiliate program (Andale Advertising), a 359-product digital storefront business (John's Guides / americanjohn.com), a contractor site with full sales-ops CRM, a 16-engine search MCP server, and an ops dashboard. Previously: built GoDaddy's Cerberus WAF (ran 14 years unchanged), scaled MSSP SOC SOAR platforms 4,000x, co-founded and sold a security data company. Stack: Laravel, Livewire, Filament, PostgreSQL, Stripe, Python, Medusa, AI/ML infrastructure. Four SOAR certifications.

Certifications

Swimlane SOAR Certified Architect, Developer, Administrator; Shuffle SOAR Certified Developer

Selected Product Work (2026)

Home Staked — two-sided marketplace SaaS (homestaked.com)

Laravel 12, Filament 3, PostgreSQL, Stripe Cashier, Reverb websockets, Horizon queues. 56K lines, 79 migrations, 172 tests.

- Identity-verified Arizona business directory: consumers search a 2.76M-row directory (materialized views, GIN trigram indexes); owners manage listings, leads, reviews, messaging, ads, and billing through a dedicated portal.
- Three Filament admin panels (super-admin, staff, company owner) with separate auth guards and policy-based authorization. Credits ledger, ads marketplace, Stripe subscription billing with webhook idempotency. Production-deployed with systemd queue and websocket services.

Andale Advertising — agency SaaS (live, andaleadvertising.com)

Laravel 11, Livewire 3, PostgreSQL, Stripe (live), ElasticEmail. 36K lines, 540 Blade views.

- Self-serve service catalog with Stripe checkout, client portal, and affiliate program (30-day referral tracking, commission ledger). Admin panel: 21 Livewire components for clients, payments, reports, affiliates, commissions, custom invoices.

John's Guides — digital product business (live, americanjohn.com)

Python, Jinja2, Medusa, Next.js, PostgreSQL, Stripe. 359 certification study guides, each researched, written, designed, and packaged as a branded PDF. Automated build pipeline (content → PDFs → catalog → storefront), two storefront builds (static generator + Medusa headless commerce), transactional mail across 6 domains.

mega-search MCP — deep search infrastructure (live)

Python, FastMCP, ~30 modules. 16 search engines (web, small-web, Anna's Archive, Wayback, open directories, face search, Shodan/Censys), 16-platform social search (Reddit with comment mining, HackerNews, YouTube, Telegram, Bluesky, Mastodon, and more), Tor onion search with maintained source catalog.

Data & Automation Infrastructure (all running daily)

- **Outreach Campaign Engine** — AI-drafted outreach gated by a 4-judge quality panel, A/B model testing, CRM integration, 1,200 sends/day with automatic suppression.
- **Proxy Infrastructure Platform** — self-hosted rotating proxy: 100+ sources, 11 protocol validations, site-affinity routing, MITM detection. Docker + systemd.

Other Shipped Work

Command Center v2 — 12-page Laravel ops dashboard (live worker monitoring, screenshot mosaic, JSON API). **Phoenix Builders** — contractor site + full sales-ops CRM backend, three iterations.

Experience

Product Platform and Design Architect – Lono Security | Remote

December 2024 – Present

- Founded the first vendor-independent SOAR professional-services and managed-platform firm. Clients get working automation in a week; the industry model is selling a gutted product then billing 6-12 months of engineer time to build it out.
- Designed a modular, serial SOAR automation model that consolidates tooling into a single core repository, letting each new integration plug in with one managed workflow and shortening time-to-value on customer deployments.
- Delivered professional-services engagements covering new SOAR builds, workflow rebuilds and data migration between platforms, customization, and customer staff training.
- Positioned clients for agentic automation by preparing data models, runbooks, and integration patterns to support future data processing, threat identification, and automated remediation workflows (readiness work — not a shipped agentic product).
- Integrated live threat-intelligence and data-enrichment tools into the SOAR via sub-automation workflows within the TI platform, keeping enrichment logic decoupled from core playbooks.

Director of Scaling – CFC Response | Remote

December 2023 – November 2024

- Designed and built out an MSSP SOC SOAR platform, taking ownership end-to-end while working 100% remotely.
- Integrated the platform with a broad third-party stack including Accelo, Sevco, SentinelOne, Huntress, Cyber Intelligence House, Polarity, Carbon Black, Stellar Cyber, OpenCTI, MISP, AlienVault, Hudu, and Torq.
- Built a deployment automation stack that provisions each client workspace as a fully separate, isolated install.
- Sized the SOAR hosting architecture to scale ~4,000x beyond the pilot's concurrent-workflow ceiling, while keeping hosting cost growth roughly flat — ~\$200K/year avoided versus scaling linearly with customer count.
- Worked with international teams to merge previously siloed per-region MDR teams onto a single platform with global 24/7 coverage.

Cybersecurity Engineer – Phoenix Cyber Security (dedicated to Swimlane SOAR) | Remote

October 2021 – July 2023

- Served as a dedicated professional-services architect on the Swimlane SOAR product, engaging directly with Swimlane's largest Fortune 500 clients.
- Built tool suites for middleware, data-management, and migration challenges across SOC platforms (EDR, XDR, SOAR, MDR, DLP, SIEM, case management).
- Customized 100+ security, ticketing, database, and service integrations through 3rd-party API and client modifications.
- Introduced Python asynchronous pipelining into workflow automation to handle higher concurrency in playbooks.
- Worked with SOC teams on IOC tracking and latent-threat detection; on targeted IOC workflows this translated to analyst manual-effort reductions of roughly 8x at peak versus the customer's prior manual triage baseline (a relative reduction on specific high-volume indicator workflows, not a uniform SOC-wide metric).

Product Platform & Design Architect and Co-Founder – Weblron / Dark Sources Security | Remote

September 2014 – August 2021

- Co-founded and ran the technical, product, and operational side of the business through to a successful company sale.
- Built a data-classifier platform that automated processing of 200+ data points per record to build detailed profiles, paired with an automated personal breach-data reporting engine and a business risk-management API.
- Recovered and held roughly 400 petabytes of stolen/breached data sets over the company's operating period (2014–2021).
- Architected a cloud-controlled web server security platform with an autonomous AI WAF engine and an on-demand cloud protection network delivering a private global CDN.
- Built a passive DNS intelligence platform monitoring ~192 million domains, and launched the first public reverse blacklist for bot automation and abusive networks (2014).
- Led pre- and post-sales engineering, closing deals with 1,000+ SME clients.

Lead Platform Engineer and Lead Hosting Security Engineer – GoDaddy | Scottsdale, AZ

2011 – 2014

- Built GoDaddy's internal shared-hosting WAF, "Cerberus", the first of its kind. GoDaddy ran it for 14 years without replacing a line of code. A company that later spun out of GoDaddy took the code and mechanics and resold them as their own product. Cerberus still runs across all GoDaddy hosting environments, blocking billions of attacks daily.
- Led the Linux Platform Engineering team hosting tens of millions of websites across thousands of servers.

- Led an overhaul of outbound hosting mail systems that substantially reduced spam. Mitigated a widespread service disruption caused by automated botnets, restoring service.
- Invited to speak at GoDaddy's internal conference on automation security; received the "Wow Me" award four times.

CTO / CIO – Internet Commerce Group | Phoenix, AZ

1998 – 2019 (full-time through ~2014; limited advisory involvement 2014 – 2019)

- Started as employee #3 (sysadmin) and grew into the technology and product leader; retained in a limited advisory capacity after 2014 as focus shifted to Weblron.
- Engineered a content management system aggregating celebrity data from 600 sources; at its peak, the system generated hundreds of millions of content pages daily as a backend for content services and marketing.
- Migrated infrastructure to redundant AWS and Google Cloud solutions; led the automation platform transformation from Chef to Puppet and the OS migration from Gentoo to CentOS.

Systems Administrator / Manager – Goodnet | Phoenix, AZ

1994 – 1998

- Designed Arizona's first shared hosting infrastructure. Before this, web hosting required an entire dedicated server per site; Goodnet was the first company in Arizona to offer shared hosting.
- Hardened ISP security when none existed: wrote scripts to parse logs for attack intelligence, added debug logging to internet-facing servers, and maintained an active TCP wrapper list to block hostile traffic.
- Built custom modem-management hardware at roughly 1/50th the cost of industry-standard devices. Managed the ISP's Cisco network infrastructure across 28 cities and a team of junior administrators.

Additional Experience

Disability Care Provider – Arion Care | Mesa, AZ

January 2026 – Present (part-time evenings)

- Part-time evening role working directly with kids with developmental disabilities, supporting daily life skills and social development.

Skills

Full-stack: Laravel (11-13), Livewire, Filament, PHP 8.2-8.3, PostgreSQL, MySQL, Stripe/Cashier, Tailwind, Vite.

Backend & Infrastructure: Python (async, Flask, FastAPI), Node.js, Redis, Docker, systemd, nginx/Apache, Caddy, Linux.

AI/ML: Ollama (local + cloud), Stable Diffusion/ComfyUI, multi-agent orchestration, LLM evaluation, MCP server development, prompt engineering.

Security & SOAR: SOAR platform design, SOC operations, SIEM (Splunk/SPL), WAF, threat intelligence, incident response, IOC tracking.

Data & Automation: ETL pipelines, web scraping at scale, data enrichment, PostgreSQL optimization, CI/CD, browser automation, email pipelines, proxy infrastructure.

Cloud: AWS, Google Cloud, VPS deployment, DNS/mail configuration.

Selected Recognition

- "Wow Me" award (4x) and distinguished internal conference speaker, GoDaddy.
- Recommendation letters on request from GoDaddy direct manager and Internet Commerce Group company owner.
- Successfully exited Weblron / Dark Sources Security via company sale.