



Aaron Gerard Davidson

CYBERSECURITY INVENTOR · AI GOVERNANCE RESEARCHER · TECHNICAL FIELD LEADER

South Lake Tahoe, CA | aaron@shapingrooms.com
shapingrooms.com | orbitauthority.com | ORCID 0009-0004-2758-9035

Useful in markets before they have stable language.

Thirty-two years in security—usually before the category had a stable name. From vulnerability management and identity to wireless, network detection, and agentic AI, the move has stayed the same: find the mechanism, learn it completely, and make it legible to buyers, engineers, and executives. Now: postural manipulation, The Atmosphere Attack, and runtime AI governance.

))) CURRENT RESEARCH & INDEPENDENT WORK	
The Atmosphere Attack Named and documented postural manipulation: semantically benign context can change an LLM's orientation before an instruction arrives. Demonstrated directional shifts across four frontier model families and propagation through three-agent chains. Published reproducible probes and a six-layer defensive architecture. DOI 10.5281/zenodo.19485192 · OWASP proposal #807 • Coordinated disclosure · Mar 2026	ORBIT: Runtime AI Governance Independent venture. A deterministic authority layer for AI systems that act: fixed policy checks, step-up approval, exact-action verification, and evidence-backed receipts before consequential execution. Early access · orbitauthority.com
Shaping the Room Constructive companion to the security research: a taxonomy of primers, posture-design methods, and an architecture for intentional human-AI interaction. DOI 10.5281/zenodo.19485354 · shapingrooms.com	Filed Patent Portfolio Filed provisional portfolio covering non-semantic governance, authority origination, delegation narrowing, execution integrity, tamper-evident receipts, and postural security. RabbitHoleSpiral LLC · Patent applications pending

))) SIGNAL ARC

Five times before the language stabilized.

INFRASTRUCTURE 1994 - 2001 Netcom and early commercial internet infrastructure. Learned to diagnose across networks, systems, applications, and people, usually before there was a playbook. Netcom · LFR Levine Fricke · Bigwords.com · EngineX Networks	THE FIRST SE 2001 - 2012 Employee #16 and first SE at nCircle. Spent more than a decade making vulnerability management legible before most buyers had the vocabulary. nCircle (acquired by Tripwire)	IDENTITY & ACCESS 2012 - 2015 Privileged identity at Xceedium; IdP, SAML, MFA, and step-up authentication at SecureAuth. Built and led a seven-person sales engineering practice. Xceedium (acquired by CA) · SecureAuth	EMERGING DOMAINS 2015 - 2019 Built the technical sales system at seven-person EvengX, then entered broadband RF and IoT at Loch with no established playbook. Investigate, test, name. EvengX (acquired by SecureSky) · Loch Technologies	NDR -> AI 2019 - present Reinvented network visibility for large Northern California enterprises at ExtraHop. In parallel: published postural manipulation research and built ORBIT's external authority model. ExtraHop · Shaping Rooms LLC · RabbitHoleSpiral LLC
1994 - 2001	2001 - 2012	2012 - 2015	2015 - 2019	2019 - present



HOW I WORK

I do not sell products that do not work; I help fix them. I do not sell to teams; I join them. Most teams know their domain better than I do. I know things they do not. We find where those intersect.

THIRTY-TWO YEARS.
SAME TRADE.