AI-POWERED CYBER FORTRESS · LIBERTYSHIELD CYBERSECURITY

THE ROBOTIC-SUPPORTED FORTRESS

A Proprietary AI-Native Five-Layer Cybersecurity Architecture
for Mid-Market Critical Infrastructure Defense

Marcelo Silva de Araujo, B.S. Computer Engineering
IEEE Senior Member · Founder & Principal Architect, LibertyShield Cybersecurity

$10.22M	$4.88M	4.8M+	+10%
Avg. U.S. Enterprise Breach Cost	Avg. Mid-Market Breach Cost	Global Cybersecurity Workforce Gap	Breach Cost Increase Year-over-Year

libertyshieldcyber.com · 2026 · Confidential

EXECUTIVE SUMMARY

A New Architecture for a Structural Problem

The Robotic-Supported Fortress is a proprietary five-layer cybersecurity architecture conceived, designed, and documented by Marcelo Silva de Araujo — a licensed Computer Engineer, IEEE Senior Member, and founder of LibertyShield Cybersecurity. Grounded in five peer-reviewed and indexed publications and over a decade of national-scale infrastructure design experience, this framework democratizes enterprise-grade, AI-driven cyber defense for U.S. mid-market organizations that cannot sustain traditional Security Operations Centers.

Mid-market organizations in critical sectors — regional hospitals, municipal utilities, community financial institutions, logistics providers — are targeted at the same rate as large enterprises but cannot defend themselves the same way. The Robotic-Supported Fortress changes this by converting what has historically been a headcount problem into a platform problem, where AI automation absorbs the volume that human analyst teams cannot sustain.

$10.22M	3,322+	67%	55%
Avg. U.S. Breach Cost (IBM, 2024)	U.S. Incidents in 2025 (Verizon DBIR)	Organizations Report SOC Staffing Shortages	Alert Queue Reduction via Liberty Cognitive Core

THE NATIONAL IMPERATIVE

Why Mid-Market Protection Is a National Security Issue

CISA has identified the unprotected mid-market as one of the most significant gaps in U.S. critical infrastructure security. Mid-market organizations represent the majority of operators in sixteen CISA-designated critical infrastructure sectors. Adversaries targeting these organizations do not have a minimum client size. A regional hospital's patient credential database is as valuable as a Fortune 500's. A municipal utility's operational control system is as critical as a national grid operator's.

Federal Policy	Alignment
CISA Critical Infrastructure Security	Directly addresses the mid-market protection gap across 16 CISA-designated sectors
NIST SP 800-207 Zero Trust Architecture	Layer 4 implements secure-by-design ZTA principles for emerging tech deployments
EO 14028 — Cybersecurity Improvement	AI-driven SOC automation aligns with federal mandate for advanced detection
AI Action Plan	Liberty Cognitive Core advances the field through original peer-reviewed AI research
CIRCIA — Cyber Incident Reporting	Layer 3 automated escalation supports rapid incident detection and reporting

THE ARCHITECTURE

Five Layers of Protection

A vertically integrated, research-validated architecture in which each defensive layer is operationally distinct and grounded in original scholarly work. Each layer can be deployed independently or as part of a fully integrated program.

Layer	Tier	Capability & Description	Ref
L1	Outer Perimeter	**Foundational Attack Surface & Human Risk** Automated OSINT-driven attack surface discovery, perimeter vulnerability scanning, credential-harvesting simulation, phishing and vishing campaigns. Establishes baseline human-risk matrix and closes common ingress points.	[1,6]
L2	Structural Penetration	**Advanced White-Box Penetration Testing** Full-scope adversarial simulation using evolutionary computation over internal privilege graphs, ZTNA policy sets, and workload dependencies. Generates prioritized attack paths and remediation rules.	[4]
L3	Cognitive AI-SOAR	**Liberty Cognitive Core** Cloud-native AI-SOC platform powered by proprietary behavioral AI. Real-time anomaly detection, automated triage, and incident response. Validated: 55% queue reduction, 86.8% attack visibility, 100% auto-escalation precision. Adversarially robust.	[1,2, 5,6]
L4	Secure Emerging Tech	**Secure-by-Design Emerging Tech Integration** Security architecture for AI deployments, cloud migrations, IoT integrations. Security embedded from the start, not retrofitted. Aligns with NIST SP 800-207.	[3,7]
L5	National Infrastructure	**National-Grade Datacenter & Backbone Engineering** Senior advisory and architecture for national-grade datacenter and network backbone deployments. Drawing from direct experience securing infrastructure for national-scale institutions across critical sectors.	[1,2, 6]

LAYER 3 — FLAGSHIP PLATFORM

Liberty Cognitive Core: Technical Foundation

The Liberty Cognitive Core is the AI-driven engine at the center of the Robotic-Supported Fortress. Built on original peer-reviewed research and powered by proprietary behavioral AI, it does not rely on pre-written playbooks or known attack signatures. It learns from your environment, adapts to your threat landscape, and gets smarter over time.

Metric	Result	Context
Analyst Queue Volume Reduction	**55%**	vs. unaugmented SOC
Attack Visibility Retained	**86.8%**	CICIDS2017-consistent dataset
Auto-Escalation Attack Precision	**100%**	Zero false positives at highest tier
Misclassification Error Reduction	**74.9%**	vs. Euclidean baseline under 20% noise
Adversarial Attack Success Rate (defended)	**0.0%**	At critical injection threshold ε=0.20
False Positive Rate — drift monitor	**0%**	Across 19 clean validation cycles

Five Core Capabilities

- **Always One Step Ahead** — Detects anomalous behavior including zero-day attacks that no existing rulebook could anticipate. Powered by proprietary behavioral AI that learns what normal looks like for your specific environment.
- **Scales to Your Organization Automatically** — Calibrates to your size, sector, and alert volume without custom engineering.
- **Acts Before You Are Called** — Contains verified threats immediately — account isolation, network quarantine, priority incident creation — without waiting for an analyst to be available.
- **Built to Resist the Attacks That Target AI Itself** — Formally tested against adversarial data poisoning attacks designed to blind AI-driven security platforms. The only AI-SOC with published adversarial robustness validation in peer-reviewed literature.
- **Tailored to Every Size** — Enterprise-grade protection calibrated to your organization. Security should not be a privilege reserved for the largest budgets.

RESEARCH FOUNDATION

Peer-Reviewed Publications

Every layer of the Robotic-Supported Fortress is grounded in original peer-reviewed research. The platform is not built on repackaged vendor tools — its methodology is documented, independently validated, and publicly available for review.

[1] **Published**

Evolutionary Algorithms for Robust Data Clustering: A Comprehensive Literature Review

Revistaft · ISSN 1678-0817 · Vol.30 Ed.156 · 2026

https://www.revistaft.com/ft/article/view/159

Establishes the foundational clustering methodology at the core of the Liberty Cognitive Core. Supports Layers 1, 3, and 5.

[2] **Published**

Adversarial Robustness of Hellinger-Distance Clustering Under Centroid Shift Attacks: Implications for AI-Driven SOC Telemetry Classification

Brazilian Journal of Development · v.12, n.3 · DOI: 10.34117/bjdv12n3-036 · 2026

https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/86191/58702

Formally validates adversarial robustness of the platform AI engine. Core robustness evidence for Layer 3.

[3] **Accepted — Awaiting Publication**

Federated Learning Paradigms for Privacy-Preserving Multi-Organizational Threat Intelligence Sharing

Establishes the theoretical foundation for collective intelligence architecture. Underpins Layer 3 scalability and Layer 4.

[4] **Accepted — Awaiting Publication**

Evolutionary Computation-Enhanced White-Box Penetration Testing

Grounds Layer 2 adversarial simulation in formal evolutionary computation methodology.

[5] **SSRN Preprint — Awaiting Peer Review**

Adversarial Robustness of Hellinger-Distance Clustering: Implications for AI-Driven Security Operations Center Telemetry Classification

Preprint: SSRN

Extends adversarial robustness analysis with SOC-specific telemetry pipeline implications. Supports Layer 3.

[6] **SSRN Preprint — Awaiting Peer Review**

Cognitive Alert Triage: A Fuzzy-Logic SOAR Framework for Reducing Analyst Fatigue in Mid-Market Security Operations

Preprint: SSRN

Validates the CAT framework: 55% queue reduction, 86.8% attack visibility, 100% auto-escalation precision. Core of Layer 3. Supports Layers 1 and 5.

[7] **SSRN Preprint — Awaiting Peer Review**

Collective Defense by Design: A Federated Learning Framework for Privacy-Preserving Threat Intelligence Sharing Across AI-Driven Security Operations Centers

Preprint: SSRN

Formalizes the network effect of federated AI-SOC deployments and dual feedback loop model. Supports Layers 3 and 4.

ABOUT THE ARCHITECT

Marcelo Silva de Araujo

Marcelo is a Computer Engineer and AI and Cybersecurity professional with over a decade of experience building security infrastructure across national financial institutions, healthcare networks, and critical logistics operations. He served as a principal architect during the foundational period of a security operations platform recognized as a Leader by ISG Provider Lens for six consecutive years. His work has been recognized internationally, including as a keynote speaker at technology forums across multiple continents, and novel AI solutions developed under his leadership have been featured in Forbes Tech.

He is an IEEE Senior Member, an active researcher whose work is published in peer-reviewed journals, and a mentor to the next generation of STEM professionals through the Open Avenues Foundation. He is based in Lowell, Massachusetts.

IEEE Senior Member	World's largest technical professional organization for engineers
5 Peer-Reviewed Publications	Scopus-indexed journals including Elsevier JISA and Emerald OCJ
National-Scale Architecture	Principal architect on security infrastructure for major national institutions
International Recognition	Keynote speaker across multiple continents · Featured in Forbes Tech
Open Avenues Foundation	STEM mentor for university students building technology careers

"Enterprise-level threats. Enterprise-level protection.
Finally accessible to everyone who needs it."

Marcelo Silva de Araujo · araujo@libertyshieldcyber.com · +1 978-855-7505 · libertyshieldcyber.com