ASHLAND, MA / GREATER BOSTON · OPEN TO DIRECTOR-LEVEL ROLES

Roger Figuereo

IT & Security Leader — Infrastructure, Security Operations, AI Governance

Fifteen years owning enterprise IT and security end to end — a decade running a $1.7M function with a team of three, today a $1.1M+ technology portfolio and a production agentic AI governance program in a business that had none.

CISSP | SECURITY+ | U.S. ARMY VETERAN | CLEARANCE-ELIGIBLE | ENGLISH / SPANISH

SCOPE LEDGER

What the title says vs. what I own

Job titles at small technology organizations rarely track accountability. This is the honest accounting of the function I currently run — the same one a hiring committee would inherit.

TITLE OF RECORD

Senior Systems & Security Administrator

NOBULL — national consumer brand, ~200 employees. May 2025 to present.

ACTUAL MANDATE

Owner of the enterprise security and systems function

~200-employee national DTC athletic brand. One direct report, a $1.1M+ annual technology budget across 15 vendor contracts, and the full security and AI governance stack.

Security posture & risk — ACCOUNTABLE

Security strategy and roadmap, technology risk assessment, vulnerability management end to end, and posture reporting to executive stakeholders.

AI governance — BUILT FROM ZERO

Four enterprise AI platforms under one framework mapped to NIST AI RMF 1.0 and ISO/IEC 42001, tiered by department need: ChatGPT and Microsoft Copilot workforce-wide, Claude for power users and code, Perplexity for research and market analysis. Authored the AI Acceptable Use Policy and the MCP Permission Policy over a 17-permission delegated access model.

Identity & access — ACCOUNTABLE

Identity lifecycle, conditional access, MFA, and SSO across the entire employee population — Microsoft 365, Entra ID, Azure, AWS — plus organization administration, role and permission models, and periodic access review for Snowflake and GitHub.

Continuity & recovery — BUILT FROM ZERO

Selected and deployed the enterprise backup and DR platform across Microsoft 365, AWS, and Google workloads, setting recoverability and retention standards that did not previously exist, backed by on-premises NAS storage.

Network & zero trust — BUILT FROM ZERO

Designed and deployed zero-trust network access from the ground up, replacing legacy VPN with brokered per-application private access and inline inspection of outbound web traffic across the workforce.

Service management & SLAs — BUILT FROM ZERO

Built the IT service management function from nothing — service desk implementation, ITIL-aligned incident, change, request, and problem workflows, and defined SLAs with measured attainment.

Vendors & MSSP — ACCOUNTABLE

A $1.1M+ annual technology budget across 15 vendor contracts — managed security services, the edge platform, and endpoint lifecycle — carried through renewal negotiation and consolidation, plus the third-party review pipeline gating every platform before procurement.

Endpoint & fleet — ACCOUNTABLE

Windows and macOS fleet management on a single co-managed stack — one plane owning enrollment, zero-touch provisioning, compliance policy, and conditional access; the other owning RMM, patching, scripting, and ticketing.

Incident response — LEAD RESPONDER

Lead responder for security and systems incidents: EDR and managed detection response, phishing triage, containment, root-cause analysis, and documented lessons learned.

NINE DOMAINS · ONE FUNCTION

SELECTED WORK

Programs I built and ran

GOVERNANCE — NOBULL

An AI governance program written before the tools shipped

Leadership wanted AI capability across the company. I built the control structure first: acceptable-use policy, a risk assessment framework, and adoption guardrails mapped to NIST AI RMF 1.0 and ISO/IEC 42001, took it through executive approval, then matched tooling to the work rather than standardizing on one vendor.

Four enterprise platforms under one framework — ChatGPT and Microsoft Copilot workforce-wide, Claude for power users and code, Perplexity for research and market analysis — deployed to 200 licensed users with identity integration and reviewed data-handling paths.

CONTINUITY — NOBULL

Recoverability where there was none

The organization had no defensible recovery position across its cloud estate. I evaluated the market, selected an enterprise backup and DR platform, and deployed it across Microsoft 365, AWS, and Google workloads with retention and recovery standards attached.

Recovery objectives defined and testable across three cloud platforms.

ZERO TRUST — NOBULL

Zero trust, stood up from nothing

Remote access ran on legacy VPN with flat internal reachability and no inline inspection of outbound traffic. I designed and deployed zero-trust network access from the ground up — policy model, application segmentation, identity integration, and phased cutover for the full workforce.

Zero-trust private access replacing VPN. Inline web security across all users.

EXPOSURE — NOBULL

A hundred counterfeit storefronts taken down

Customer-facing commerce properties were exposed at the edge and the brand was being counterfeited at scale. I run the takedown program against storefronts trading on the name, and architected the WAF and DDoS protection standing behind it.

100+ counterfeit storefronts removed. The perimeter absorbed 60 DDoS attacks over 12 months and now turns away 46% of inbound traffic as malicious.

SERVICE DELIVERY — NOBULL AND ELKUS MANFREDI

Service management, built from nothing — twice

Both organizations ran IT support on inbox and hallway requests, with no ticket record and no agreed response times. At each, I implemented the service desk, defined ITIL-aligned incident, request, change, and problem workflows, and negotiated service-level agreements with the business.

SLA attainment measured and reported. Support demand visible for the first time at both firms.

THIRD-PARTY RISK — NOBULL, ELKUS MANFREDI, SMB CLIENTS

A security gate in front of every vendor

Software gets bought by the department that wants it, and security finds out at renewal. I built the same pipeline three times over — intake, vendor security questionnaire, SOC 2 and evidence review, data-handling and access scoping — ending in a documented risk-acceptance decision before anything is signed.

Vendor risk decided before procurement, not discovered after. Built at enterprise, firm, and SMB scale.

SELECTED WORK

Continued

PRINCIPAL CONSULTANT / VCISO — INDEPENDENT PRACTICE

The security executive for firms that could not hire one

Small law practices and nonprofits carrying real exposure with no in-house security function. I built their environments from zero and served as their security executive — setting direction, aligning to security and compliance requirements, then pressure-testing with leadership tabletops and penetration testing.

Four organizations brought into compliance alignment. Exploitability proven rather than assumed, with risk-ranked remediation and retest validation.

CONSOLIDATION — NOBULL

Two endpoint stacks collapsed into one

Devices were managed across overlapping tools with no single source of enrollment truth. I retired the redundant MDM and merged the survivors into one co-managed stack — one plane owning enrollment, zero-touch provisioning, compliance policy, and conditional access; the other owning RMM, patching, scripting, and ticketing.

$12K in annual recurring license spend eliminated and machine sprawl ended, with zero end-user downtime.

MIGRATION — ELKUS MANFREDI ARCHITECTS

300 mailboxes moved without an outage

A 300-user professional services firm on aging on-premises Exchange, with zero tolerance for downtime during active project deadlines. I planned and executed the cutover to Microsoft 365 alongside the change management and training to make it stick.

Zero downtime, on schedule, 300+ mailboxes migrated.

COST — ELKUS MANFREDI ARCHITECTS

Twenty percent out of the operating cost line

Ten years owning the IT budget and vendor portfolio for the firm. I redesigned service processes, automated recurring work, and renegotiated the vendor stack against what the business actually consumed.

Approximately 20% reduction in technology operating cost.

PLATFORM — NOBULL

Agent infrastructure with identity underneath it

Agents are only as safe as the access they hold. I wrote the internal MCP servers brokering agent access to Snowflake, GitHub, Slack, and Azure Container Apps — Entra ID External OAuth, per-role token acquisition via managed identity, a three-tier autonomy model, and an audit evidence layer. It runs on Azure Container Apps, the managed Kubernetes-based platform, with every environment defined as infrastructure as code in Terraform and Bicep, network security groups segmenting it, and CI/CD doing the deploys — secrets held in 1Password and injected at deploy rather than committed to source. I administer and govern the Snowflake and GitHub organizations those servers reach into.

Delegated agent access that survives an audit rather than merely functioning. Plus an executive BI command center with Snowflake as single source of truth.

LEADERSHIP — U.S. ARMY

Thirty people, five thousand users, three deployments

Led Signal and Cyber Operations teams across domestic bases and three overseas sites, accountable for training, readiness, performance, and career development — while owning the communications and information systems the mission ran on, including the deployed comms Civil Affairs teams operated on for partner-nation and interagency missions.

Zero mission-impacting outages. Training programs cut user-driven incidents 35%.

OPERATING RANGE

Where I work

IDENTITY & SECURITY

Entra ID, Conditional Access, Zscaler ZIA/ZPA, Microsoft Defender XDR, Huntress MDR, CrowdStrike Falcon, Cloudflare WAF and Zero Trust, Rapid7, Microsoft Purview, Metasploit.

GOVERNANCE & COMPLIANCE

ISO/IEC 27001, SOC 2 Type II, NIST CSF 2.0, CIS Controls, FedRAMP, FISMA, HIPAA, NIST AI RMF 1.0, ISO/IEC 42001. Vanta. Policy authorship, control design, evidence collection, auditor engagement, third-party risk.

CLOUD & DATA

Azure (primary) — Container Apps, Terraform and Bicep, managed identity, network security groups and segmentation. Snowflake and GitHub (organization administration and access governance), Cloudflare Workers, AWS (supporting).

AI & AUTOMATION

Multi-platform enterprise AI administration — Claude, ChatGPT, Microsoft Copilot, Perplexity. MCP server development, infrastructure as code (Terraform and Bicep), CI/CD build and deploy pipelines, secrets management in 1Password, TypeScript, PowerShell, Microsoft Graph API.

ENDPOINT & CONTINUITY

Microsoft Intune, NinjaOne, Intune + NinjaOne co-management, Autopilot, Windows and macOS fleet management. Commvault, NetApp, Synology NAS.

PLATFORMS

Microsoft 365, Freshservice, Shopify, Snowflake, Slack, Asana, Tableau. Cisco Meraki firewall, SD-WAN, switching, wireless.

SECURITY OPERATIONS

Vulnerability management at 5,000-endpoint scale, perimeter defense and takedowns, penetration testing with Metasploit, incident response tabletops, conditional access.

TRACK RECORD

Fifteen years

2025 – Present

Senior Systems & Security Administrator

NOBULL — Boston, MA

Senior IT and security owner for a ~200-employee national DTC athletic brand. One direct report, a $1.1M+ annual technology budget across 15 vendor contracts, and the full security and AI governance stack: identity and access, zero-trust network access, endpoint detection and managed response, unified endpoint management, edge protection, and enterprise backup and recovery.

2023 – 2025

Principal Consultant / vCISO

Independent IT & Cybersecurity Consulting — Greater Boston

Acting security executive for four clients — small law practices and nonprofits with no in-house security function. Built greenfield environments from zero, set security direction, brought each into alignment with security and compliance requirements, and ran leadership tabletops and penetration testing with Metasploit. Ran concurrent with the Education Development Center role from June 2024.

2024 – 2025

Information Security Analyst III

Education Development Center — Waltham, MA

Security operations and tooling ownership across a 5,000-machine estate. Triaged 100,000+ alerts annually on the Rapid7 platform and hardened the environment to FedRAMP, FISMA, ISO/IEC 27001, SOC 2, and HIPAA control requirements.

2013 – 2023

IT Manager

Elkus Manfredi Architects — Boston, MA

IT and security function owner for a 300-person architecture and design firm: three direct reports all hired in seat, MSP partner oversight, the full vendor portfolio, and a $1.7M annual budget. $300K in recurring annual savings; led the firm to ISO/IEC 27001 certification and SOC 2 Type II attestation, implementing Vanta for continuous compliance monitoring.

2010 – 2019

Signal and Cyber Operations

United States Army — Active Duty & Reserve

Reserve service ran concurrent with the civilian role. Three combat deployments. Led up to 30 personnel across communications and cyber operations, and delivered the systems Civil Affairs teams operated on for partner-nation and interagency missions.

EDUCATION & CREDENTIALS

Certified and cleared

EDUCATION & TRAINING

- U.S. Army Signal (25-series) technical training — communications systems and network operations
- U.S. Army Cyber Operations (17-series) technical training — cyber defense

SECURITY & GOVERNANCE

- CISSP — Certified Information Systems Security Professional
- CompTIA Security+
- OWASP SAMM Fundamentals
- Clearance — previously held during Army service; eligible for sponsorship and reinvestigation

AI & CLOUD

- Claude Certified Architect
- Microsoft Certified — Azure AI Engineer Associate
- AWS Certified — AI Practitioner
- Google Cloud — Professional Machine Learning Engineer

SERVICE

- Army Commendation Medal
- Army Achievement Medal (multiple)
- National Defense Service Medal
- Afghanistan Campaign Medal
- Global War on Terrorism Service Medal

LANGUAGES

- English — native / bilingual
- Spanish — native / bilingual

Let's talk about scope

I'm open to director-level technology and security leadership roles in Greater Boston and remote-friendly organizations nationally. The fastest way to reach me is email.

EMAIL	**Figuereo.Roger@Outlook.com**
PHONE	**(857) 991-7277**
LINKEDIN	**/in/rogerfiguereo**
PORTFOLIO	**rogerfiguereo.com**