Roger Figuereo

CISSP | IT & Security Leadership · Team & Budget Ownership · Infrastructure · Security Operations · AI Governance

Ashland, MA 01721 | (857) 991-7277 | Figuereo.Roger@Outlook.com | linkedin.com/in/rogerfiguereo | rogerfiguereo.com

PROFESSIONAL SUMMARY

IT and security leader with 15+ years owning enterprise technology functions end to end — strategy, roadmap, budget, vendors, team, and security posture. Currently the senior owner of technology and security for a 200-employee national consumer brand, directing a $1.1M+ portfolio across 15 vendor contracts. Previously ran a $1.7M IT function for a decade with a team of three hired and developed in seat plus managed-provider oversight, delivering $300K in recurring annual savings and leading the firm to ISO/IEC 27001 certification and SOC 2 Type II attestation. Builds the functions that did not previously exist — cybersecurity, disaster recovery, service management and SLAs, and an AI governance framework mapped to NIST AI RMF 1.0 and ISO/IEC 42001 adopted by the executive team. CISSP and CompTIA Security+ certified, with applied AI credentials across Azure, AWS, and Google Cloud. Fifteen years of progressive technical and leadership experience in lieu of a bachelor's degree. Bilingual in English and Spanish.

CORE COMPETENCIES

Multi-Year IT Strategy & Technology Roadmap • Team Leadership, Hiring & Development • Budget Ownership & Vendor Negotiation • Executive & Stakeholder Management • Cybersecurity Strategy & Risk Management • Security Governance, Policy & Standards • AI Governance & Responsible AI • Identity & Access Management • Vulnerability & Threat Management • Incident Response • Disaster Recovery & Business Continuity • Multi-Site Infrastructure • Endpoint & MDM Management • Third-Party Risk & Vendor Security Assessment • Team Leadership & MSP/MSSP Oversight • IT Governance, KPIs & Service Metrics • Compliance (SOC 2 Type II, ISO/IEC 27001, NIST CSF 2.0, NIST AI RMF 1.0, ISO/IEC 42001, CIS Controls, HIPAA)

PROFESSIONAL EXPERIENCE

Senior Systems & Security Administrator

May 2025 – Present

NOBULL — Boston, MA · national direct-to-consumer athletic brand, ~200 employees

Senior owner of the enterprise technology and security function. Scope: 1 direct report plus managed security services partner, $1.1M+ annual technology budget across 15 vendor contracts, full technology roadmap.

- Direct the 15-contract vendor portfolio behind the $1.1M+ budget — managed security services, the enterprise edge platform, and endpoint lifecycle among them — through renewal negotiation, consolidation, and risk-based investment decisions.
- Serve as the organization's senior security authority — set strategy and roadmap, assess technology risk, and report posture, exposure, and remediation priorities to executives.
- Established the enterprise AI governance program from the ground up — acceptable-use policy, risk assessment framework, delegated-access permission model, and adoption guardrails mapped to NIST AI RMF 1.0 and ISO/IEC 42001, adopted by the executive team ahead of any user-facing rollout. Rolled out and administer four enterprise AI platforms under it, tiered deliberately by department need rather than standardized on one tool — ChatGPT and Microsoft Copilot workforce-wide, Claude for power users and code, Perplexity for research and market analysis — each with identity-bound access, license management, and its own data-handling review.
- Architected and maintain the enterprise edge security tier — WAF, DDoS mitigation, and zero-trust access — for global workloads and customer-facing services: 60 DDoS attacks mitigated in 12 months, 46% of inbound traffic filtered as malicious, ~72.7M bot requests blocked monthly, and 100+ counterfeit storefront takedowns protecting brand IP.
- 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 workforce-wide.
- Built the third-party security review pipeline from the ground up — intake, vendor questionnaires, SOC 2 evidence review, data-handling and access scoping, and documented risk-acceptance decisions gating every new platform before procurement.
- Executed the endpoint management consolidation: retired a redundant MDM and merged the survivors into 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 — cutting $12K in annual license spend and ending machine sprawl with zero end-user downtime.
- Lead disaster recovery and business continuity — evaluated the market, selected and deployed the enterprise backup and DR platform across Microsoft 365, AWS, and Google workloads, establishing recoverability and retention standards where none existed, backed by on-premises NAS for local restore.
- Own vulnerability management end to end and serve as lead responder for security and systems incidents — EDR and managed detection response, phishing triage, containment, root-cause analysis, and periodic access reviews, aligned to SOC 2 Type II and NIST CSF 2.0.
- Built the IT service management function and SLAs from the ground up (ITIL-aligned service desk), and cut onboarding and offboarding from three days to one through automation across Microsoft Graph, Slack, and serverless edge workers.
- Administer and govern the Snowflake and GitHub organizations — configuration, identity-bound SSO access, role and permission models, and periodic access review — and wrote the internal MCP servers brokering agent access to them under per-role, identity-bound tokens, shipped through CI/CD with secrets held in 1Password and injected at deploy time rather than committed to source.

Principal Consultant

September 2023 – May 2025

Independent IT & Cybersecurity Consulting — Greater Boston, MA

Acting security executive (vCISO) for legal and nonprofit clients with no in-house security function. Ran concurrent with the EDC role from June 2024.

- Built greenfield client environments from zero — tenant setup, Entra ID and Microsoft 365 configuration, NinjaOne RMM and endpoint management, device enrollment and imaging, patch policy, backup, and remote access — with documented runbooks and administrative handoff, then retained steady-state scope.
- Hardened client environments as part of every build: MFA and Conditional Access enforcement, endpoint protection deployment, backup and recovery testing, and least-privilege access design.
- Facilitated cyber incident response tabletop exercises with leadership teams, pressure-testing escalation paths, decision-making, and communications against realistic breach scenarios.
- Performed penetration testing with Metasploit, delivering exploitability findings, risk-ranked remediation guidance, and retest validation.
- Stood up vendor security assessment and third-party risk processes for clients with no procurement security function, advising on tooling selection, access controls, and Microsoft 365 hardening with roadmaps mapped to NIST CSF and CIS Controls.

Information Security Analyst III
June 2024 – March 2025

Education Development Center (EDC) — Waltham, MA · federally funded research organization

- Ran vulnerability management across a 5,000-machine estate, triaging 100,000+ alerts annually through the Rapid7 platform and driving patch and configuration remediation to closure with system owners.
- Executed risk assessments, vulnerability testing, and security audits against NIST CSF, CIS Controls, ISO/IEC 27001, SOC 2, and HIPAA control requirements, strengthening organizational compliance posture.
- Led investigations and end-to-end incident response, presenting root-cause analysis and remediation plans to senior leadership.
- Built security awareness training that measurably improved phishing resistance, and partnered with engineering to embed security requirements into the software development lifecycle.

IT Manager
April 2013 – September 2023

Elkus Manfredi Architects LTD — Boston, MA · 300-person professional services firm

Scope: 3 direct reports plus outsourced MSP, full vendor portfolio, $1.7M annual IT budget.

- Led a three-person team — every member hired, onboarded, and developed in seat — and directed an outsourced managed service provider; set standards, escalation paths, and ticket-handling practice, and owned hiring, performance management, and career development.
- Managed the full vendor portfolio and a $1.7M annual IT budget, delivering $300K in recurring annual savings through consolidation and renegotiation, and directing multi-year modernization with executive stakeholders.
- Platform owner for a hybrid Azure and Microsoft 365 environment serving ~300 users across a decade — full accountability for infrastructure, endpoints, identity, service delivery, and the technology roadmap.
- Led the firm to ISO/IEC 27001 certification and SOC 2 Type II attestation, owning control design, evidence collection, and auditor engagement; implemented Vanta for continuous compliance and vendor risk monitoring.
- Delivered a zero-downtime migration from Exchange Server 2019 to Microsoft 365, moving 300+ mailboxes on schedule with no business disruption.
- Directed change management and firm-wide training, cutting operating cost ~20%; reduced monthly security alert volume 20% through tuning, endpoint hardening, and root-cause remediation.
- Established the firm's vendor security assessment process, its service management function and SLAs, and the identity, endpoint, and system hardening standards adopted firm-wide.

Lead Security Analyst & Signal Operations Leader
October 2010 – January 2019

United States Army — Active Duty & Reserve

Reserve service ran concurrent with the civilian role.

- Led and developed ~30 personnel across Signal (25-series) and Cyber Operations (17-series) teams, including three combat deployments — responsible for training, readiness, performance, and career development.
- Owned mission-critical communications and information systems supporting 5,000+ users across domestic bases and three overseas sites, maintaining zero mission-impacting outages.
- Enforced information assurance requirements, access controls, classified media handling, and configuration standards under governing military security policy.
- Delivered the deployed communications and information systems Civil Affairs teams operated on for partner-nation and interagency missions.
- Briefed senior leadership on system performance, operational risk, and security posture; designed technical training that reduced user-driven incidents by 35%.

TECHNICAL SKILLS

Security Operations	Microsoft Defender XDR, Huntress MDR, CrowdStrike Falcon, Rapid7, Microsoft Purview (DLP & data governance), Zscaler ZIA/ZPA, Cloudflare (WAF, DDoS, DNS, Zero Trust), penetration testing (Metasploit), vulnerability management, MFA/SSO/Conditional Access
Governance & Compliance	SOC 2 Type II, ISO/IEC 27001, NIST CSF 2.0, CIS Controls, HIPAA, NIST AI RMF 1.0, ISO/IEC 42001, OWASP Top 10, Vanta, third-party risk management, vendor security assessment, policy authorship, tabletop exercises
Endpoint & MDM	Microsoft Intune, NinjaOne (RMM, patching, scripting, ticketing), NinjaOne + Intune co-management, Kandji, Autopilot, Windows and macOS fleet management, baseline and configuration profiles, application packaging
Identity & Cloud	Entra ID (Azure AD), Microsoft 365, Exchange Online, SharePoint & OneDrive, Conditional Access, group policy · Azure — Azure Container Apps (managed Kubernetes-based platform), infrastructure as code with Terraform and Bicep, managed identity, network security groups and segmentation · AWS (supporting)
Platforms & Network	Snowflake and GitHub (organization administration, role and permission governance, access review), Shopify, Freshservice, Asana, Tableau · Cisco Meraki firewall, SD-WAN, switching, wireless · multi-site branch connectivity, VPN and remote access
Continuity & Storage	Commvault (enterprise backup and DR across Microsoft 365, AWS, and Google workloads), NetApp enterprise storage (replication, DR), Synology NAS
Service Management	ServiceNow and Freshservice (ITIL-aligned), NinjaOne ticketing, SLA design and attainment reporting, Jira
Reporting & Automation	PowerShell, TypeScript, Terraform, Bicep, Microsoft Graph API, Power Automate, Cloudflare Workers, infrastructure as code, CI/CD build and deploy pipelines, secrets management (1Password, injected into Git workflows and Azure Container CLI deploys), Model Context Protocol (MCP) server development, multi-platform enterprise AI administration — Claude, ChatGPT, Microsoft Copilot, Perplexity

CERTIFICATIONS, EDUCATION & RECOGNITION

Security & Governance	CISSP — Certified Information Systems Security Professional • CompTIA Security+ • OWASP SAMM Fundamentals
AI & Cloud	Claude Certified Architect • Microsoft Certified: Azure AI Engineer Associate • AWS Certified AI Practitioner • Google Cloud Professional Machine Learning Engineer
Education & Training	U.S. Army technical and leadership training — Signal (25-series) and Cyber Operations (17-series); fifteen years of progressive technical and leadership experience in lieu of a bachelor's degree.
Clearance & Service	U.S. Army veteran — previously held a U.S. government security clearance, eligible for sponsorship and reinvestigation • Army Commendation Medal • Army Achievement Medal (multiple) • National Defense Service Medal • Afghanistan Campaign Medal • Global War on Terrorism Service Medal
Languages	English and Spanish (native/bilingual)