CLINT E. BODUNGEN

AI/ML Engineering Leader · Agentic AI Architect · OT/ICS Cybersecurity Pioneer

Author of "ChatGPT for Cybersecurity Cookbook" and "Hacking Exposed: Industrial Control Systems" · Creator of ThreatGEN® Red vs. Blue and AutoTableTop™

clint@bodungen.ai · linkedin.com/in/clintb

AI/ML engineering leader who designs and ships production agentic-AI systems — multi-agent architectures, retrieval-augmented generation, security knowledge graphs, and LLM evaluation frameworks — backed by a 30-year cybersecurity career spanning OT/ICS security, red teaming, and vulnerability research. Currently Director of AI/ML Engineering at Arcova, leading the team behind AI-native cybersecurity and GRC platforms, and Founder of ThreatGEN, where I created the world's first online multiplayer cybersecurity simulation game and an autonomous AI incident-response exercise platform. U.S. Air Force veteran and author of two best-selling cybersecurity books, with prior roles at Kaspersky Lab, Booz Allen Hamilton, and Symantec. My work sits where AI engineering and security operations meet: systems that don't just assist analysts, but plan, build, reason, and simulate alongside them.

CORE COMPETENCIES

AI / ML Engineering · Multi-agent system architecture (LangChain / LangGraph) · Retrieval-augmented generation (RAG) · Structured & constrained generation · Tool-using autonomous research agents · LLM-as-judge evaluation & AI-efficacy testing frameworks · Provider-abstracted multi-model integration (Anthropic, OpenAI, local models) · Semantic embeddings & vector similarity · Knowledge graphs (Neo4j, natural-language-to-Cypher) · Agentic coding & AI workflow orchestration · LLM cost optimization

AI Security & Governance · Secure agentic-AI integration · Human-in-the-loop control design · Source provenance & confidence tracking · Deterministic fallback architecture · AI-native GRC and third-party risk workflows

Cybersecurity · OT/ICS & SCADA security · Vulnerability research and 0-day discovery · Penetration testing & red teaming · Risk assessment and analysis · Enterprise risk management programs · Threat intelligence · Regulatory and standards compliance · Security architecture

Engineering & Platforms · Python · TypeScript / JavaScript · C / C++ / C# · Cypher & SQL · Linux shell · Unity3D & game-engine simulation · Behavior trees and utility-based game AI · Digital twins / VR cyber ranges

Leadership · Engineering team leadership · AI-native product strategy · Product ownership & roadmap · Startup founding and fundraising · Technical evangelism and public thought leadership

PROFESSIONAL EXPERIENCE

Arcova (formerly MorganFranklin Cyber) · Remote — **Aug 2024 – Present**

Director, AI/ML Engineering — *Aug 2025 – Present*

- Lead the AI/ML engineering team building production agentic-AI applications across cybersecurity and GRC — including an AI-powered third-party risk management platform (automated vendor tiering, trust-center evidence mapping, OSINT and dark-web risk monitoring), an AI change-management intake system, and LLM-powered go-to-market and sales-intelligence tools.
- Architect multi-agent and LLM systems using retrieval-augmented generation (RAG), structured and constrained generation, tool-using research agents, and provider-abstracted multi-model integration across Anthropic, OpenAI, and locally hosted models.
- Established a multi-layer AI-efficacy testing framework — including LLM-as-judge evaluation — as an engineering release gate that measures whether AI features actually perform, not merely whether the code runs.
- Advise on the secure integration of agentic AI: human-in-the-loop controls, source provenance and confidence tracking, and deterministic fallbacks.
- Drive AI-native product strategy, reframing document-heavy GRC workflows around AI ingestion and inference layers that draft analysis directly from evidence with per-field provenance.

Director, Cybersecurity Innovation — *Aug 2024 – Aug 2025*

- Led an innovation engagement delivering an AI-powered vulnerability-management platform for a critical-infrastructure security client, fusing enterprise assets, NVD vulnerabilities, MITRE ATT&CK and D3FEND, and CISA KEV exploit intelligence into a Neo4j security knowledge graph queryable in natural language.
- Designed a multi-agent AI layer in LangChain and LangGraph: natural-language-to-Cypher graph querying, RAG-based security chatbots, and a self-extending meta-agent that writes its own graph analytics from plain-English use cases.

- Built an exploit-aware, four-layer AI asset-deduplication engine — deterministic fingerprinting, semantic-embedding similarity, graph adjacency, and LLM adjudication — that cut LLM cost roughly 70% through cheapest-method-first tiering.

ThreatGEN (Derezzed, Inc.) · Houston, TX **Jun 2017 – Present**

Founder / Chairman / Head of Product Innovation

- Founded a venture-funded cybersecurity company closing the industry skills gap through gamification and AI-driven training, built on modern game engines, simulation technology, and generative AI/LLMs.
- Creator of ThreatGEN AutoTableTop™, an AI-powered incident-response tabletop exercise platform driven by a multi-agent LLM system — an AI facilitator, scenario and timeline agents, and dynamic inject delivery — with structured outputs and real-time orchestration.
- Co-creator of ThreatGEN® Red vs. Blue, the world's first online multiplayer game-based cybersecurity simulation, including its adversarial red-team/blue-team game AI: utility-based behavior trees with animation-curve utility scoring plus an exploratory neural-network opponent, since re-engineered for the web in TypeScript.
- Creator and developer of the ThreatGEN VR ICS/OT digital-twin cyber range.
- Author and lead instructor of the ThreatGEN Red vs. Blue OT Cybersecurity Masterclass; deliver custom cybersecurity games and gamification solutions for enterprise clients.
- Pioneered applied generative AI and LLM use across cybersecurity training, exercises, and real-world operations — spanning game AI, autonomous exercise facilitation, and AI-assisted content generation.

LEO Cyber Security · Houston, TX **Oct 2017 – Jan 2019**

Executive Vice President, ICS Cyber Security

- Built the ICS cybersecurity business practice from the ground up — directing its vision and philosophy, establishing strategic partnerships, identifying technological opportunities, and recruiting senior industry talent.
- Served as the firm's key ICS cybersecurity subject-matter expert, providing pre-sales support and public thought leadership.

Kaspersky Lab, North America · Houston, TX **May 2016 – Sep 2017**

Senior Researcher, Critical Infrastructure Threat Analysis

- Principal technical ICS subject-matter expert for Kaspersky globally; researched and analyzed emerging ICS threats and vulnerabilities and coordinated vulnerability disclosure with vendors and DHS ICS-CERT.
- Researched and developed cutting-edge applications, tools, and technology for industrial control system security.
- Served as the public ICS voice of the brand in North America — approving ICS media releases, giving press interviews, and presenting at industry conferences; instructor and presenter at multiple ICS cybersecurity workshops at MIT.

Booz Allen Hamilton · Houston, TX **Feb 2015 – May 2016**

Senior Industrial Cybersecurity Researcher / Analyst

- Led and performed ICS security risk assessments and penetration testing engagements.
- Lead architect of the Probabilistic Risk Assessment Model (PRAM) and technical developer for the firm's ICS security predictive analytics.
- ICS security SME supporting business development, proposals, and marketing; authored whitepapers and presented at industry conferences.

Cimation (acquired by Accenture) · Houston, TX **Jul 2013 – Jan 2015**

R&D Manager, Cyber Security Solutions / Senior ICS-SCADA Security Researcher

- Performed ICS/SCADA 0-day vulnerability research and discovery, malware analysis, IDS signature development, proof-of-concept exploit development, penetration testing, and vulnerability assessments.
- Principal architect and developer of Cimation's threat intelligence and vulnerability feed interface; principal contributor to the threat intelligence program's business model and strategic roadmap.
- Program architect, principal course developer, and lead instructor for Cimation University, the company's online ICS/SCADA cybersecurity training program.
- Authored the company's vulnerability assessment and penetration testing standard operating procedures and methodologies.

Gas Certification Institute, LLC · Houston, TX · Contract **Feb 2008 – Feb 2019**

SCADA Security Instructor & Course Developer

- Authored and taught SCADA cybersecurity courses over an eleven-year instructional engagement.

North American University · Houston, TX · Contract — **Aug 2016 – Jan 2017**

Adjunct Professor

- Taught CS 3325 — Computer Network Security; faculty leader of the Computer Science Club.

Amor Group (a Lockheed Martin company) · Houston, TX — **Sep 2011 – Jul 2013**

Senior Security Consultant / Analyst

- Led cyber, physical, and operational security vulnerability assessments, penetration tests, red-team exercises, risk assessments, and regulatory gap analyses for ICS/SCADA environments as team lead and project manager.
- Helped clients build and maintain ICS/SCADA security and risk management programs; recommended and deployed mitigation strategies and technologies including SIEM.
- Maintained the security lab for threat analysis, vulnerability and exploit research, product evaluation, and training; published multiple ICS/SCADA security whitepapers.

CIDG, Corp. · Houston, TX — **Jan 2008 – Sep 2011**

Founder / Principal Security Analyst

- Co-founder of CiSACS (Comprehensive Industrial Security and Compliance Solution).
- Delivered security vulnerability assessments, penetration testing, red-team testing, risk assessments, and compliance gap analyses for ICS/SCADA environments as team lead and project manager.
- Supported business development and sales for vendor technologies; published multiple ICS/SCADA security whitepapers.

Industrial Defender (formerly PlantData Technologies) · Houston, TX — **Nov 2004 – Jan 2008**

SCADA Security Consultant

- Developed security auditing tools and standardized testing methodology across the company's consulting services.
- Performed penetration testing and risk/vulnerability assessments and implemented mitigation strategies and security policies for some of the world's largest energy, utility, oil & gas, and communications companies.
- Tested Emerson DeltaV controllers for security vulnerabilities on-site at Emerson.

Diverse Networks, Inc. · Houston, TX — **Nov 2003 – Nov 2004**

SCADA Security Consultant

- Performed penetration testing and risk/vulnerability assessments and implemented security policies for major energy, utility, oil & gas, and communications companies.
- Implemented security mitigation and remediation for Chevron-Texaco's RTAP SCADA systems and developed a secure remote wireless alarm solution for controllers on the Chevron-Texaco Pipeline SCADA network.

First Community Services · Killeen, TX — **Aug 2002 – Nov 2003**

Vice President, IT Security · Chairman, Disaster Recovery Committee

- Built and led the IT security team responsible for security administration, maintenance, and testing across more than 200 bank branches; owned the department budget, policies, and procedures.
- Renegotiated the disaster recovery contract with a new vendor, increasing recovery capability while saving $1.7M annually.
- Developed an in-house detection tool for viruses and worms engineered to evade IDS and anti-virus, preventing major outbreaks including Bugbear.b.

Symantec Corporation · San Antonio, TX · Contract — **Feb 2002 – Aug 2002**

SQA Engineer, Network Intrusion Detection Systems

- Developed IDS software, quality assurance tests, and attack signatures for the Symantec Net Prowler IDS.
- Built lab systems and networks simulating attacks and intrusions for IDS testing; taught the CISSP preparation course to Symantec employees.

SynchroNet, Inc. · Houston, TX — **Oct 1999 – Feb 2002**

Vice President, Security Operations

- Helped build the information security department from the ground up — technology R&D, hiring and training, and policy and procedure design.
- Engineered and developed a proprietary packet-filtering firewall, VPN, and IDS network appliance with a web-based configuration interface, deployed across multiple client sites.
- Delivered network security solutions nationally: firewall deployment, risk analysis, vulnerability assessments, penetration testing, IDS implementation, and custom security software development.

United States Air Force · Barksdale AFB, LA **Apr 1995 – Oct 1999**

Computer Systems Security Officer (CSSO) / OPSEC Manager

- Responsible for squadron-level IT security and flight-level OPSEC; developed disaster recovery and contingency plans, information security policies, and training procedures.
- Performed base-wide risk analysis, vulnerability assessments, and penetration tests during contingency exercises and while deployed for Operation Southern Watch (Saudi Arabia) and Operation Desert Strike (Diego Garcia).
- Supported computer-crime investigations in coordination with other government organizations.

PUBLICATIONS

ChatGPT for Cybersecurity Cookbook

Packt Publishing, March 2024 · ISBN 978-1805124047 · Best seller

Hacking Exposed: Industrial Control Systems — ICS/SCADA Security Secrets & Solutions

McGraw-Hill, September 2016 · ISBN 978-1259589713 · Principal author · Best seller

RECOGNITION & AFFILIATIONS

- Founding Fellow — Control System Cyber Security Association International, $(CS)^2AI$ (2020 – Present)
- Author of two best-selling cybersecurity books (McGraw-Hill, Packt Publishing); course creator and conference presenter for Packt
- Creator of the PCIP (Professional in Critical Infrastructure Protection) certification program
- Instructor and presenter, ICS cybersecurity workshops at MIT
- United States Air Force veteran
- Frequent keynote and conference speaker on OT/ICS security, applied generative AI, and agentic systems

EDUCATION

Game Institute 2014 – Present

Game design and programming coursework: C#/C++, Unity3D, artificial intelligence, mathematics for game physics, 3D graphics and game-engine programming, 3D art and animation, electronics and robotics.

Louisiana Tech University — Barksdale AFB, LA 1997 – 1999

Coursework in Computer Science.

Community College of the Air Force — Barksdale AFB, LA 1997 – 1999

Coursework in Information Technology / Computer Science.

Colorado Institute of Art — Denver, CO 1993 – 1995

Associate of Applied Arts, Industrial Design Technology.