

Technical Capabilities & Experience

Dr. Stephen Dietrich-Kolokouris, PhD | CCIE | Cybersecurity · AI/ML Systems · Data Engineering · Strategic Analysis

This document provides a comprehensive overview of technical capabilities, project experience, toolchain proficiency, and domain expertise. It is intended to support recruiter and hiring manager evaluation across cybersecurity, AI/ML engineering, data engineering, network architecture, and strategic analysis roles.

Last updated: February 2026 | Distribution: Professional use

1. Cybersecurity & Offensive Security

Over 15 years of cybersecurity experience spanning intelligence community contracting, enterprise security architecture, penetration testing, incident response, and independent security research. Certified CCIE with deep hands-on experience across the full attack lifecycle — from reconnaissance and initial access through lateral movement, persistence, exfiltration, and post-incident forensics.

1.1 Penetration Testing & Red Team Operations

Extensive experience conducting authorized offensive security engagements against enterprise networks, web applications, wireless infrastructure, and operational technology (OT) environments. Engagements have ranged from black-box external assessments to full-scope red team exercises with physical and social engineering components.

- Network penetration testing: external perimeter, internal pivoting, Active Directory attack chains (Kerberoasting, AS-REP roasting, DCSync, Golden Ticket, Silver Ticket, Pass-the-Hash, NTLM relay)
- Web application testing: OWASP Top 10, server-side request forgery (SSRF), insecure deserialization, JWT manipulation, OAuth/OIDC misconfiguration, API abuse, GraphQL introspection, business logic flaws
- Wireless: WPA2-Enterprise EAP downgrade attacks, evil twin AP deployment, PMKID capture, Bluetooth Low Energy (BLE) sniffing against IoT devices
- Social engineering: phishing campaign design and execution, pretexting, vishing, physical tailgating, USB drop attacks, callback phishing
- OT/ICS: Modbus TCP reconnaissance, SCADA protocol fuzzing, PLC ladder logic analysis, network segmentation validation for Purdue Model compliance
- Cloud: AWS/Azure/GCP configuration review, IAM policy analysis, S3 bucket enumeration, Lambda function injection, metadata service exploitation (IMDS v1/v2), Azure AD enumeration

1.2 Penetration Testing Toolchain

- Reconnaissance: Nmap, Masscan, Shodan, Censys, Amass, Subfinder, theHarvester, OSINT Framework, SpiderFoot, Maltego, Recon-ng
- Exploitation: Metasploit Framework, Cobalt Strike, Sliver C2, Havoc C2, Covenant, custom Python/Go implants, Impacket suite, CrackMapExec, BloodHound/SharpHound, Rubeus, Mimikatz, Certify/Certipy (AD CS attacks)
- Web: Burp Suite Pro, OWASP ZAP, SQLMap, ffuf, Gobuster, Nuclei, httpx, Arjun (parameter discovery), Postman/Insomnia for API testing
- Wireless: Aircrack-ng, Kismet, Bettercap, WiFi Pineapple, HackRF One for SDR
- Post-exploitation: PowerShell Empire (legacy), BOF (Beacon Object Files), Seatbelt, SharpUp, LaZagne, Chisel/ligolo-ng for tunneling, WinPEAS/LinPEAS
- Reporting: custom LaTeX templates, Ghostwriter, Dradis, PlexTrac

1.3 Incident Response & Digital Forensics

Led and supported incident response engagements across ransomware, business email compromise (BEC), advanced persistent threat (APT) intrusions, and insider threat investigations. Experienced in both reactive IR (containment, eradication, recovery) and proactive threat hunting.

- Forensic acquisition: FTK Imager, KAPE, dc3dd, Magnet ACQUIRE, live memory capture with WinPmem/LiME, chain-of-custody documentation
- Analysis platforms: Autopsy, X-Ways Forensics, Volatility 3 (memory forensics — process injection detection, rootkit hunting, credential extraction), Plaso/log2timeline for super-timeline generation
- Log analysis: Splunk (SPL), Elastic/Kibana (KQL), Graylog, Chainsaw (Windows EVTX rapid triage), Hayabusa, Sigma rule authoring, YARA rule development
- Network forensics: Wireshark/tshark (deep packet analysis, TLS fingerprinting with JA3/JA4), Zeek (formerly Bro) for connection logs and protocol analysis, NetworkMiner, Arkime (full packet capture at scale)
- Malware analysis: static analysis with PE-bear/CFF Explorer/Ghidra, dynamic analysis in isolated VMs with Process Monitor, API Monitor, Cuckoo Sandbox, behavioral detonation with Any.Run and Joe Sandbox
- Ransomware response: negotiation support, decryptor assessment, Bitcoin/Monero transaction tracing with Chainalysis Reactor, recovery coordination, lessons-learned documentation

1.4 Threat Intelligence & Hunting

- MITRE ATT&CK; framework: mapped TTPs for APT28, APT29, APT41, Lazarus Group, FIN7, and Sandworm during intelligence analysis work; developed detection rules aligned to technique IDs
- Threat hunting: hypothesis-driven hunts in Splunk/Elastic using behavioral analytics, frequency analysis (stacking), long-tail analysis for C2 beaconing detection, DNS tunneling identification
- Intelligence platforms: MISP, OpenCTI, Recorded Future, VirusTotal Enterprise, Shodan Monitor, GreyNoise
- Attribution analysis: infrastructure correlation (WHOIS, passive DNS, certificate transparency logs), malware family classification, campaign tracking

1.5 Security Architecture & Governance

Designed and reviewed security architectures for enterprise, critical infrastructure, and government environments. Experience aligning technical controls to compliance frameworks and business risk tolerance.

- Zero Trust architecture design: microsegmentation (Illumio, Guardicore), identity-centric access (Okta, Azure AD Conditional Access, BeyondCorp), continuous verification, least-privilege enforcement
- Network security: next-gen firewall policy (Palo Alto, Fortinet, Cisco Firepower), IDS/IPS tuning (Suricata, Snort), WAF configuration (Cloudflare, AWS WAF, F5), DDoS mitigation
- Endpoint: CrowdStrike Falcon, SentinelOne, Carbon Black, Microsoft Defender for Endpoint — EDR deployment, tuning, custom detection rules
- Email security: Proofpoint, Mimecast, Microsoft Defender for Office 365 — anti-phishing, DMARC/DKIM/SPF enforcement, attachment sandboxing
- Compliance frameworks: NIST CSF, NIST 800-53, NIST 800-171, CMMC, ISO 27001, SOC 2 Type II, PCI DSS, HIPAA Security Rule, FedRAMP
- Risk assessment: quantitative risk modeling (FAIR methodology), threat modeling (STRIDE, PASTA, attack trees), business impact analysis, risk register management
- Security program development: security roadmap creation, policy authoring, security awareness training program design, vendor risk management (third-party security assessments, SIG questionnaires)

2. Network Engineering & Architecture (CCIE)

CCIE-certified network engineer with deep implementation experience across enterprise campus, data center, WAN, service provider, and cloud networking environments. Hands-on from physical layer through application-layer optimization.

2.1 Routing & Switching

- BGP: full-table eBGP peering, route reflector design, BGP community-based traffic engineering (local-pref, MED, AS-path prepending), BGP Flowspec for DDoS mitigation, BGP RPKI for route origin validation, confederation design for large-scale ISP networks, graceful restart and BFD integration
- OSPF: multi-area design (stub, NSSA, totally stubby), LSA filtering, summarization at ABR, OSPF virtual links, OSPFv3 for IPv6, SPF tuning for convergence optimization in large campus networks (1000+ routers)
- IS-IS: single-topology and multi-topology deployment in SP environments, IS-IS segment routing integration, TI-LFA (Topology Independent Loop-Free Alternate) for sub-50ms failover
- EIGRP: stub routing, variance-based unequal-cost load balancing, named mode configuration, EIGRP-to-OSPF mutual redistribution with loop prevention (route tags, distribute lists)
- MPLS: LDP and segment routing (SR-MPLS), MPLS TE with RSVP-TE, L3VPN (VPNv4/VPNv6), L2VPN (VPLS, EVPN-MPLS), inter-AS MPLS VPN (Option A/B/C), MPLS QoS with EXP bit marking
- Multicast: PIM-SM, PIM-SSM, MSDP for inter-domain multicast, IGMP snooping optimization, multicast in MPLS VPN (MDT), Rendezvous Point redundancy with Anycast RP and MSDP

2.2 Data Center Networking

- VXLAN/EVPN: BGP EVPN control plane with VXLAN data plane, distributed anycast gateway, multi-site EVPN with border gateway design, EVPN Type-2 (MAC/IP), Type-5 (IP prefix) route handling, silent host detection, ARP suppression
- Spine-leaf architecture: Clos fabric design, ECMP load balancing, leaf-spine oversubscription ratio planning, breakout cable management, fabric capacity planning for East-West traffic patterns
- Cisco ACI: tenant/VRF/BD/EPG policy model, contract design, L4-L7 service graph insertion (firewalls, load balancers), multi-pod and multi-site ACI, ACI integration with VMware vCenter and Kubernetes
- VMware NSX: NSX-T distributed firewall micro-segmentation, T0/T1 gateway design, NSX-T federation for multi-site, overlay transport zone design, NSX Advanced Load Balancer (Avi) integration
- Arista: Arista EOS, CloudVision (CVP), MLAG, EVPN-VXLAN on Arista 7500R/7280R platforms, Arista DMF for network packet broker/TAP aggregation
- Storage networking: Fibre Channel (16/32Gbps), FCoE, NVMe-oF, iSCSI, storage VLAN design, jumbo frame configuration and MTU path verification

2.3 WAN & SD-WAN

- SD-WAN: Cisco Viptela (vManage/vSmart/vBond/vEdge), Fortinet SD-WAN, VMware VeloCloud — hub-and-spoke and full-mesh topologies, application-aware routing, SLA-based path selection, DIA/DCA breakout
- Traditional WAN: DMVPN (Phase 1/2/3 with NHRP), GRE/IPsec, FlexVPN (IKEv2), GETVPN for multicast-capable encrypted WAN, WAN optimization with Cisco WAAS and Riverbed SteelHead
- QoS: end-to-end QoS design (classification at access, queuing at WAN edge), DSCP marking, LLQ for voice, CBWFQ, shaping vs policing, QoS pre-classify for tunnel interfaces
- Internet edge: dual-homed BGP with ISP, prefix-based outbound traffic engineering, inbound TE with BGP communities, RTBH (Remotely Triggered Black Hole) for DDoS, DNS-based GSLB

2.4 Wireless & Campus

- Cisco wireless: WLC 9800 (IOS-XE), Catalyst 9100 series APs, FlexConnect, Cisco DNA Center (now Catalyst Center) for automation and assurance, 802.11ax (Wi-Fi 6/6E) deployment, RF planning with Ekahau
- Campus design: routed access layer (Layer 3 to the edge), VSS/StackWise Virtual for distribution, SDA (Software-Defined Access) with ISE and TrustSec SGT, macro/micro segmentation
- Network access control: Cisco ISE (RADIUS, TACACS+, 802.1X, MAB, profiling, posture assessment, guest portal, BYOD onboarding), ClearPass, Microsoft NPS

2.5 Network Automation & Observability

- Automation: Ansible (network modules for IOS, NX-OS, EOS, JunOS), Terraform (AWS VPC, Azure VNet), Python (Netmiko, NAPALM, Nornir, Scrapli), REST API integration with DNA Center/vManage/ACI APIC
- CI/CD for network: Git-based config management, pre-commit linting (Batfish for config validation), automated testing with pyATS/Genie, Containerlab for topology simulation
- Observability: SNMP polling (LibreNMS, Zabbix), streaming telemetry (gNMI, gRPC), NetFlow/sFlow/IPFIX analysis (Plixer Scrutinizer, ntopng, Kentik), Grafana/InfluxDB dashboards, ThousandEyes for SaaS/Internet path monitoring

3. AI/ML Systems & LLM Engineering

Designed and deployed production retrieval-augmented generation (RAG) systems, AI-powered automation agents, and data-driven analytics pipelines. Focus on systems that are evidence-constrained, auditable, and operationally reliable.

3.1 RAG Architecture & Vector Search

Built multiple production RAG systems for domain-specific Q&A, document analysis, and decision support. End-to-end ownership from document ingestion through embedding, retrieval, generation, and output guardrails.

- Document processing: PDF/DOCX/HTML ingestion, OCR pipeline for scanned documents (Tesseract, Amazon Textract), recursive text splitting with semantic chunk boundary detection, metadata preservation (source, page, section heading)
- Embedding models: OpenAI text-embedding-ada-002 and text-embedding-3-small/large, Sentence Transformers (all-MiniLM-L6-v2, BGE-large), Cohere embed-v3, embedding dimension reduction and quantization for cost optimization
- Vector databases: FAISS (flat, IVF, HNSW indexes — index selection based on corpus size and latency requirements), Pinecone (managed, serverless), Weaviate, ChromaDB, pgvector (Postgres extension for hybrid SQL+vector queries)
- Retrieval strategies: MMR (Maximal Marginal Relevance) for diversity, hybrid search (BM25 + dense retrieval with reciprocal rank fusion), contextual compression, parent-child document retrieval, multi-query retrieval with query decomposition, re-ranking with cross-encoders (Cohere Rerank, BGE-reranker)
- Evaluation: RAGAS framework (faithfulness, answer relevancy, context recall, context precision), custom evaluation harnesses with human-in-the-loop, A/B testing of retrieval configurations, chunk size optimization experiments

3.2 LLM Integration & Prompt Engineering

- Models: OpenAI GPT-4o, GPT-4-turbo, GPT-3.5; Anthropic Claude 3.5 Sonnet, Claude 3 Opus; open-source via Ollama/vLLM (Llama 3, Mixtral, Mistral); model selection based on latency/cost/capability tradeoffs
- Frameworks: LangChain (chains, agents, tools, callbacks, memory), LlamaIndex (index types, query engines, sub-question decomposition), Haystack, custom orchestration layers in Python
- Prompt engineering: few-shot and chain-of-thought prompting, system prompt design for role-constrained behavior, output format enforcement (JSON mode, structured outputs), guardrail prompts to prevent hallucination and scope drift
- Agents: tool-calling agents with function definitions, multi-step planning agents (ReAct pattern), browser automation agents (Playwright + LLM), agentic RAG with iterative retrieval and self-correction
- Guardrails: output validation regex, content filtering, source attribution enforcement, confidence thresholds, fallback behavior design ('not in documentation' responses), PII detection and redaction in outputs

3.3 MLOps & Deployment

- Serving: FastAPI endpoints for RAG services, Streamlit for interactive demos and internal tools, Gradio, Docker containerization, deployment on AWS (ECS, Lambda) and Streamlit Community Cloud
- Monitoring: token usage tracking, latency monitoring, retrieval quality metrics, cost dashboards, error rate alerting, LangSmith for trace debugging
- Cost optimization: embedding caching, response caching for repeated queries, model routing (smaller model for simple queries, larger for complex), batch processing for offline workloads

3.4 Computer Vision & Other ML

- Image classification and object detection using pre-trained models (YOLO, ResNet), transfer learning with PyTorch, OpenCV for preprocessing
 - NLP: text classification, named entity recognition, sentiment analysis using transformers (Hugging Face), spaCy for production NLP pipelines
 - Time series: anomaly detection in network telemetry and security logs using statistical methods and isolation forests
-

4. Supply Chain Security & Critical Infrastructure

Independent security researcher focused on hardware/firmware supply chain vulnerabilities in critical infrastructure. Published research on Chinese sleeper malware threats to U.S. infrastructure. Developed deterministic risk scoring models for vendor evaluation.

4.1 Supply Chain Risk Analysis

- Developed quantitative supply chain risk scoring methodology covering: firmware integrity (OTA update mechanisms, code signing, secure boot attestation), rare earth element dependency (magnet sourcing, single-supplier risk), SBOM availability and completeness, remote administration exposure, telemetry/data exfiltration vectors
- Vendor assessment: hardware teardown analysis (X-ray, decapping for IC verification), firmware extraction and reverse engineering (binwalk, JTAG/SWD debug interfaces), component provenance verification, counterfeit detection
- Threat modeling for supply chain: nation-state implant scenarios (hardware trojans, firmware backdoors), interdiction points in logistics chains, vulnerability windows in component lifecycle
- Frameworks: NIST SP 800-161 (Supply Chain Risk Management), C-SCRM, Executive Order 14028 compliance, CISA supply chain risk assessment guidance

4.2 Critical Infrastructure Focus Areas

- Energy sector: NERC CIP compliance assessment, OT/IT convergence security, SCADA/DCS/RTU protocol security (Modbus, DNP3, IEC 61850, IEC 104), substation automation security
- Water/wastewater: PLC security assessment, remote access vulnerability analysis, network segmentation between IT and OT
- Telecommunications: 5G infrastructure security assessment, RAN and core network trust boundaries, SS7/Diameter protocol vulnerability analysis
- Research output: published analysis on Chinese sleeper malware targeting critical infrastructure firmware, focusing on pre-positioned access in industrial control systems and network equipment

4.3 Deterministic Scoring Engine

Designed and implemented a deterministic supply chain risk scoring system with weighted factors for firmware risk, rare earth exposure, single-point-of-failure analysis, and geopolitical risk. The scoring engine produces tiered risk classifications with automated mitigation playbooks mapped to each tier. Deployed as a Python module with Streamlit frontend for interactive vendor comparison.

5. Data Engineering & Pipeline Development

Experience building data ingestion, transformation, and analytics pipelines for security telemetry, document processing, and operational intelligence. Comfortable across the full stack from raw data acquisition through serving layers and visualization.

5.1 Pipeline Architecture

- ETL/ELT: Apache Airflow for orchestration, dbt for transformation logic, custom Python ETL pipelines, batch and streaming architectures
- Streaming: Apache Kafka (producer/consumer design, topic partitioning strategy, Kafka Connect for source/sink integration), Redis Streams for lightweight pub/sub
- Data formats: Parquet, Avro, JSON Lines, CSV normalization, schema evolution handling, data validation with Pydantic and Great Expectations

5.2 Databases & Storage

- Relational: PostgreSQL (advanced — CTEs, window functions, JSONB, full-text search, partitioning, pgvector extension), MySQL, SQLite for embedded applications
- NoSQL: MongoDB (aggregation pipeline, indexing strategy, sharding), Redis (caching layers, rate limiting, session management), Elasticsearch (index lifecycle management, custom analyzers, KQL)
- Data warehousing: Snowflake, BigQuery, Redshift — schema design, materialized views, query optimization, cost management
- Object storage: S3 (lifecycle policies, event notifications, cross-region replication), Azure Blob Storage, MinIO for on-prem S3-compatible storage

5.3 Data Analysis & Visualization

- Python: Pandas, NumPy, SciPy for statistical analysis, Matplotlib/Seaborn for static visualization, Plotly/Dash for interactive dashboards
 - BI tools: Grafana (Prometheus, InfluxDB, Elasticsearch datasources), Tableau, Power BI, custom Streamlit dashboards
 - Geospatial: GeoPandas, Folium, Leaflet.js, geospatial analysis for threat intelligence and infrastructure mapping
-

6. Software Engineering & Development

6.1 Languages

- Primary: Python (advanced — asyncio, type hints, decorators, context managers, metaclasses, packaging with pyproject.toml, testing with pytest)
- Working proficiency: JavaScript/TypeScript (Node.js, Express, React), Go (CLI tools, concurrent network scanners), Bash/Shell scripting (advanced — system automation, log processing)
- Familiarity: Rust (security tooling), C (firmware analysis, exploit development), PowerShell (Active Directory automation, forensic scripting)

6.2 DevOps & Infrastructure

- Containers: Docker (multi-stage builds, security hardening, distroless base images), Docker Compose for local development, Kubernetes (deployment, services, ingress, RBAC, network policies, Helm charts)

- CI/CD: GitHub Actions (custom workflows, matrix builds, security scanning), GitLab CI, Jenkins, ArgoCD for GitOps
- Infrastructure as Code: Terraform (AWS, Azure, GCP providers — VPC/VNet design, IAM, compute, storage), Ansible (playbooks for server hardening, network device config), Pulumi
- Cloud: AWS (VPC, EC2, ECS, Lambda, S3, RDS, IAM, CloudWatch, GuardDuty, Security Hub), Azure (Virtual Networks, AD, Sentinel, Key Vault), GCP (Compute Engine, Cloud Functions, BigQuery)
- Monitoring: Prometheus/Grafana stack, ELK stack (Elasticsearch, Logstash, Kibana), Datadog, PagerDuty integration, custom alerting pipelines

6.3 Version Control & Collaboration

- Git: branching strategies (GitFlow, trunk-based), code review workflows, monorepo management, pre-commit hooks, conventional commits, release automation with semantic versioning
- Documentation: technical writing for architecture decision records (ADRs), runbooks, threat models, API documentation (OpenAPI/Swagger), Markdown-based project documentation

7. Intelligence Community & Defense Experience

Former CIA contractor with operational experience during Al-Qaeda and ISIS campaigns. Work included intelligence analysis, secure communications infrastructure, and technical collection support. Current defense work focuses on conflict simulation modeling.

7.1 Intelligence Operations (CIA Contractor)

- Provided technical support for intelligence operations during the Al-Qaeda and ISIS threat periods, including secure network architecture for field operations, communications security (COMSEC) planning, and technical collection infrastructure
- Network security auditing for classified environments: SCIF compliance verification, air-gap enforcement, TEMPEST considerations, SIPRNet/JWICS connectivity requirements
- Cross-domain solutions: assessment and configuration of data diodes and cross-domain transfer systems, policy enforcement for classification level boundaries
- Worked in compartmented programs requiring TS/SCI access and adherence to IC security policies (ICD 503, CNSSI 1253)

7.2 WarSim Algorithm — Conflict Simulation Model

Designed and developed the WarSim Algorithm, a deterministic conflict simulation model submitted to the Department of Defense. The system models force-on-force engagements with variable parameters for terrain, logistics, force composition, technological capability, and decision-making latency.

- Data modeling: entity-attribute framework for military units (capabilities, readiness, logistics state, morale factors), terrain effects matrix, weather impact modeling
- Simulation engine: turn-based resolution with probability-weighted outcome trees, Monte Carlo simulation for uncertainty quantification, sensitivity analysis for key variables
- Visualization: interactive scenario dashboard (Streamlit), geographic overlay using Folium/Leaflet, force disposition mapping, logistics flow visualization
- Validation: historical scenario backtesting against known conflict outcomes, subject matter expert review, parameter sensitivity documentation

7.3 National Exercise Simulation Platform

Developed a DHS-format national exercise simulation platform for tabletop exercises and full-scale exercise planning. The platform generates exercise scenarios, injects, and evaluation criteria aligned to HSEEP (Homeland Security Exercise and Evaluation Program) methodology.

8. Selected Project Portfolio

8.1 Evidence-Only Recruiter Proxy (RAG System)

- Full-stack RAG application deployed on Streamlit Community Cloud: PDF ingestion, FAISS vector store with SHA-256 manifest-based cache invalidation, MMR retrieval, GPT-4o generation with evidence-only guardrails
- Features: automatic recruiter context extraction, history-aware query rewriting, action modes (verify, fit summary, outreach draft), PDF transcript export, personal/technical tone toggle
- Stack: Python, LangChain, OpenAI, FAISS, Streamlit, ReportLab

8.2 Supply Chain Risk Scoring Platform

- Deterministic risk scoring engine for vendor/component evaluation across firmware integrity, rare earth dependency, geopolitical risk, and single-point-of-failure metrics
- Tiered classification with automated mitigation playbooks, interactive comparison dashboard, CSV-based vendor import
- Stack: Python, Pandas, Streamlit

8.3 YouTube Script Generator System

- AI-powered content pipeline for generating long-form video scripts in specific content domains (paranormal investigation, true crime, historical analysis)
- Multi-stage generation: research aggregation, outline generation, script drafting with tone/style control, SEO metadata generation
- Stack: Python, OpenAI API, custom prompt chains

8.4 Browser Automation Agents

- LLM-powered browser automation using Playwright for web research, data collection, and task automation
- Agent architecture with tool-calling, error recovery, and structured output extraction

8.5 NAMECOMMS — Neural Anomaly Manifold Entropy Communication System

- Experimental research system for anomaly detection in communication patterns, developed in collaboration with consciousness research program
 - Signal processing pipeline with entropy analysis, pattern recognition, and statistical validation
-

9. Certifications & Education

Education

- PhD — Goethe University Frankfurt (History). Dissertation focused on analytical methodology applicable to intelligence analysis, pattern recognition in complex systems, and strategic decision modeling.
- Ongoing professional development: SANS coursework, Offensive Security training, cloud security certifications, AI/ML specialization courses

Certifications

- CCIE (Cisco Certified Internetwork Expert) — Expert-level validation of network design, implementation, and troubleshooting across enterprise and service provider environments
- Additional certifications and training in penetration testing, incident response, cloud security, and forensic analysis maintained through continuous professional development

Publications

- Seven published books: Chicago Ripper Crew: Reboot (true crime), Behind the Mask: Hitler the Socialite (historical analysis), The American Paranormal (consciousness research), and four additional titles
 - Independent security research publications on Chinese sleeper malware in critical infrastructure and supply chain firmware vulnerabilities
 - WarSim Algorithm documentation submitted to Department of Defense
-

10. Work Style, Leadership & Communication

Effective in both individual contributor and technical leadership roles. Comfortable presenting to C-suite executives, government officials, and technical peers. Strong written communication evidenced by published books, research papers, and technical documentation.

- Technical leadership: architecture reviews, design document authorship, mentoring junior engineers, technical interview design and execution
- Cross-functional collaboration: experience bridging security, engineering, operations, and executive teams; translating technical risk into business impact language
- Communication: published author (7 books), media appearances (Fox 4 Dallas), comfortable with public speaking, technical writing, and executive briefings
- Remote/hybrid effectiveness: extensive experience in distributed teams, asynchronous communication, documentation-first culture, timezone-aware collaboration
- Cleared environment experience: comfortable with compartmented programs, need-to-know restrictions, classification handling, and the operational constraints of classified work

This document is maintained by Dr. Stephen Dietrich-Kolokouris and intended for professional evaluation purposes. For verification of specific claims, contact via LinkedIn.