JAYCE HILL

Principal AI Security Architect
Washington, DC · (202) 409-4788 · jayce@hillsecadvisors.com · linkedin.com/in/jaycehilleng

EXECUTIVE SUMMARY

AI Security Architect and strategist who helps Fortune 100 organizations deploy AI at scale without compromising security posture. One of a small number of practitioners who has actually built, secured, and governed agentic AI systems — including MCP server architectures, autonomous multi-agent workflows, and continuously validated AI security planning — in production across regulated industries. At Microsoft ISE, co-led the build and deployment of CRISP, a proprietary threat modeling framework operating as an MCP server, across ~20 Fortune 100 engagements, and served as a key Security Lead for HVE-Core, an Agentic platform with 34 autonomous agents available as a public repository on Microsoft's GitHub. Translates complex AI risk into practical security architecture that enables delivery velocity rather than constraining it — a model proven at Dow, Halliburton, LSEG, Bank of America, Fidelity, General Motors, KPMG, and FIS. Previously held TS/SCI CI-Poly Full Scope Lifestyle clearance.

CORE COMPETENCIES

- Agentic AI Security & Autonomous Workflow Governance
- AI/ML Security (LLM, RAG, MCP, Inference Pipelines)
- Cloud Security Architecture (Azure, AWS, OCI)
- Threat Modeling (CRISP, STRIDE, MITRE ATT&CK)
- DevSecOps & CI/CD Hardening (CodeQL, SAST/DAST)
- Software Supply Chain (SBOM, SLSA, Sigstore, SHA Pinning)
- Human-in-the-Loop Security for AI Systems
- Zero Trust Architecture & Identity Governance (Entra ID, PIM)
- Infrastructure as Code Security (Bicep, Terraform, Policy-as-Code)
- Secure SDLC & Application Security (OWASP, OpenSSF)
- Governance Automation & Compliance (RMF, NIST 800-53, FedRAMP)
- Customer Delivery & Security Enablement (Fortune 100)

TECHNICAL SKILLS

Platforms: Azure (Solutions Architect Expert), AWS, Oracle Cloud Infrastructure
Languages: Python, C#, PowerShell, Bash, Bicep
AI & Agentic Security: CRISP MCP, HVE-Core (34-agent RPI platform), Defender for AI, prompt integrity controls, tool-use boundary enforcement, human-in-the-loop validation patterns
Security Tooling: CodeQL, Defender for Cloud, Sentinel, Trivy, CycloneDX, Sigstore/Cosign, GitHub Advanced Security
Frameworks: OWASP, MITRE ATT&CK, NIST 800-53, RMF, SLSA, OpenSSF Scorecard, Zero Trust, STRIDE

PROFESSIONAL EXPERIENCE

Principal Security Software Engineer | Microsoft — Industry Solutions Engineering *2021 – Present*

Forward deployed security architect embedded with Fortune 100 and public sector customers. Security Lead for ISE's agentic AI engineering platform. Led through influence and embedded partnership — no direct reports. Level 65 (Principal).

- Served as a key Security Lead for HVE-Core; an Agentic engineering platform with 34 autonomous agents executing Research-Plan-Implement workflows via GitHub Copilot, available as a public repository on Microsoft's GitHub. Defined security boundaries for agent tool-use, established governance patterns for autonomous code generation, and led deployment workshops at KPMG (New Jersey) and LSEG (London).
- Co-led the build and deployment of CRISP, a proprietary threat modeling framework operating as an MCP server — scans customer architectures, generates data attribute tables, and produces security plans drawing from OWASP, Microsoft standards, and industry frameworks. Identified by ISE leadership as a top-priority accelerator.
- Deployed CRISP across ~20 Fortune 100 engagements including Dow, Halliburton (Helios), LSEG, Bank of America, Fidelity, General Motors, KPMG, and FIS — embedded directly in customer engineering sprints using a discuss/build/upskill model.
- Designed an AI-assisted continuous security validation workflow at Halliburton/Helios — combining CRISP MCP with HVE-Core to regenerate and validate security plans as architecture evolved weekly, reducing the planning cycle from weeks to approximately one hour per iteration while maintaining human-in-the-loop oversight for regulatory interpretation and risk prioritization.
- Architected security controls for LLM pipelines, RAG architectures, and AI inference infrastructure across regulated customer environments, addressing prompt injection, data exfiltration, model integrity, and agent autonomy boundaries.

- Hardened the CI/CD and software supply chain for the CRISP MCP accelerator — CodeQL SAST integration, workflow token permission tightening, GitHub Actions SHA pinning, Trivy container scanning expansion, CycloneDX SBOM generation and signing, and base image digest pinning. Aligned to OpenSSF Scorecard standards.
- Built a secure-by-default Bicep library spanning 11 Azure services (AKS, SQL, Cosmos, Key Vault, Redis, AI Foundry, Storage, VNet, NSG, PIM, Guardrails) with Zero Trust defaults: private networking, managed identity, and least-privilege role assignments enforced at the infrastructure layer.
- Produced customer-specific security gap analyses for KPMG, FIS, and Halliburton/Helios with end-to-end regulatory traceability — mapping regulation to gap to Bicep module to commit — establishing a reusable methodology adopted across engagements.
- Built deterministic scoring and golden-snapshot regression protection for the SPaM security analysis engine, ensuring reproducible, verifiable outputs for downstream security decisions in production environments.
- Traveled to LSEG London for the HVE Hackathon; led the Solution Architecture Design process investigation and presented at the Science Fair. Produced an 8-section SAD Submission Readiness Checklist adopted as a reusable cross-engagement artifact.

Information System Security Manager | General Dynamics IT (GDIT) *2020 – 2021*

Security operations and compliance in classified environments. TS/SCI CI-Poly Full Scope Lifestyle clearance supporting IC missions.

- Managed security accreditation (ATO) and RMF activities for classified and cloud-based systems across AWS and Azure, coordinating technical, compliance, and stakeholder workstreams.
- Conducted architecture reviews and Technical Exchange Meetings with program leadership to assess risk posture, define controls, and align remediation milestones across IC programs.
- Executed cyber security improvement strategies including post-incident analysis for data spills and zero-day vulnerability resolution.

Senior Principal Consultant — National Security Group | Oracle *2011 – 2020*

Lead security consultant across a 9-year engagement — OCI architecture, penetration testing, SDLC security, and executive program governance for national security customers.

- Served as Oracle Cloud Infrastructure Solution Architect, designing deployment architectures and leading certification and accreditation frameworks for national security programs.
- Led penetration testing and vulnerability assessments using MITRE ATT&CK across Oracle Exadata, Big Data Appliance, WebLogic, and Analytics platforms.
- Managed full project lifecycle including hardware/software integration, security testing, and end-to-end solution delivery within customized cybersecurity environments.
- Facilitated quarterly stakeholder reviews and bi-monthly Technical Exchange Meetings covering performance, risk, emerging technology, and program milestones.
- Produced System Security Plans, CONOPs, whitepapers, and risk matrices guiding program-level accreditation outcomes.

EDUCATION

M.S. Cybersecurity (in progress) — Georgia Institute of Technology
M.Eng., Systems Engineering — George Washington University
B.S., Electrical & Computer Engineering — Michigan State University

CERTIFICATIONS & SECURITY CLEARANCE

- Microsoft Azure Solutions Architect Expert
- GIAC Security Essentials (GSEC)
- Certified Ethical Hacker (CEH)
- HashiCorp Terraform Associate
- TS/SCI CI-Poly — Full Scope Lifestyle (Previously Held; Reinstatement Eligible)

SELECTED CLIENT ENGAGEMENTS

Fortune 100 & Strategic Accounts: Dow · Halliburton (Helios) · LSEG · Bank of America · Fidelity · General Motors · KPMG · FIS · U.S. Federal & IC Agencies