Brandyn Schult

brandyn@thalient.ai ❖ Irvine, CA ❖ (949) 490-0614

SECURITY CLEARANCE

Top Secret, SCI Eligible — U.S. Department of Defense

WORK EXPERIENCE

Thalient Cybernetics — **January 2023 – Present**
Co-Founder — *Irvine, CA*

- implementing NIST AI 100 and MITRE ATLAS strategies for AI safety and security, managing risks in AI systems by focusing on unique AI vulnerabilities and adversarial machine learning (AML), and developing AI safety protocols to enhance defenses against AI threats.

Supernal — **July 2022 – Present**
Lead Platform Security Engineer — *Irvine, CA*

- Leading a security engineering team performing airworthiness security (RTCA DO-326A, DO-356A) for Supernal's autonomous eVTOL aircraft, coordinating with Integrated Product Teams, and conducting Threat Assessment and Remediation Analyses.
- Conducting Model-Based Systems Engineering (MBSE) activities, including use case development, requirement decomposition, and architecture modeling, utilizing 3DExperience, Cameo Systems Modeler, Teamwork Cloud, and DOORS Next Generation.

F-35 JSF Joint Program Office — **October 2021 – July 2022**
Principal Security Architect — *Fort Worth, TX*

- SETA Architecture lead for the F-35 JSF Joint Program Office's Cyber Directorate, focused on the development of cyber capabilities for the F-35 Air Vehicle and collaborated with international partners on system security, mission assurance, and risk management
- Served as the primary cybersecurity expert, coordinating with the OEM, suppliers, and international partners on system security, software assurance, and risk management for the F-35 program.

Lockheed Martin — **July 2018 – October 2021**
Manager, Cyber Security Engineering — *Fort Worth, TX*

- Spearheaded Cyber Resiliency initiatives for Lockheed Martin's Skunkworks and F-35 JSF program, creating the F-35 Cyber Strategy, and performing the security engineering activities for the Technology Refresh (TR-3).
- Led systems engineering and design activities intended to deter and delay exploitation of critical technologies in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

Boston Cybernetics Institute — **July 2018 – March 2019**
Senior Security Researcher — *Cambridge, MA*

- Specialized in cybersecurity research; actively modeled threats, identified vulnerabilities, and mitigated risks in complex systems.

Massachusetts Institute of Technology Lincoln Laboratory — **January 2015 – June 2018**
Associate Staff — *Lexington, MA*

- Spearheaded initiatives in cyber resiliency and survivability of weapon systems and led research in secure cyber-physical systems and cybersecurity systems analysis.
- Collaborated on advanced methodologies, including Cyber Mission Thread Analysis and Mission-Based Cyber Risk Assessment, while also conducting safety-centric cybersecurity analyses for key defense projects using techniques like STAMP and STPA.

Booz Allen Hamilton — **June 2014 – December 2014**
Lead Cyber Security Engineer — *McLean, VA*

- Cybersecurity Lead for Pentagon industrial control, power plant, and Chemical, Biological, Nuclear, and Explosive (CBRNE) systems.

Department of Homeland Security — **May 2013 – September 2013**
Cyber Security Engineer — *Arlington, VA*

- Internship at the National Cybersecurity and Communications Integration Center (NCCIC).

EDUCATION

Air Force Institute of Technology — **September 2022**
Systems Engineering, Graduate Certificate — *Wright-Patterson Air Force Base*

University of Maryland Baltimore County — **December 2013**
Cyber Security, M.S. — *Baltimore, MD*

College of the Atlantic — **January 2010**
Human Ecology, B.A. — *Bar Harbor, ME*

https://www.thalient.ai/ https://www.linkedin.com/in/bschult

CERTIFICATIONS

CISSP	Certified Information Systems Security Professional	(ISC)2	449871
ASEP	Associate Systems Engineering Professional	INCOSE	289361
OCSMP	OMG-Certified SysML Professional, Model User	OMG	506097
CEH	Certified Ethical Hacker	EC-Council	Expired
CRISC	Certified in Risk and Information Systems Control	ISACA	Expired
CISA	Certified Information Systems Auditor	ISACA	Expired
Security+	CompTIA Security+	CompTIA	Expired

TRAINING

Advanced Security	Introduction to Hardware Hacking and Reverse-Engineering
Advanced Security	Introduction to RF and Software-Defined Radio (SDR)
KU Jayhawk	Aircraft Certification and Airworthiness Approvals
KU Jayhawk	Fundamental Avionics
KU Jayhawk	System Safety Assessment for Commercial Aircraft
RTCA	DO-178C – Software Considerations in Airborne Systems
RTCA	DO-326A – Airworthiness Security
Delligatti Associates	OCSMP Accelerator SysML

PRESENTATIONS

IEEE	Trustworthy Autonomy in Advanced Air Mobility
INCOSE	Performing RTCA DO-326A aircraft cybersecurity assessments using MBSE and SysML

ORGANIZATIONS

INCOSE	International Council on Systems Engineering	Member
ISC2	International Information System Security Certification	Member
ISO	International Organization for Standardization	Member
RTCA	Radio Technical Commission for Aeronautics	SC-216, Aeronautical Systems Security
USMC	United States Marine Corps Cyber Auxiliary	Systems Security Volunteer

INTERESTS

Cybernetics & Artificial Intelligence

Passionate about exploring the intersection of cybernetics and AI (see personal website https://thalient.ai). Exploring effective ways to leverage generative AI as a force multiplier in systems and security engineering. Focused on utilizing formal methods and runtime assurance techniques to establish trustworthy autonomy in cyber-physical systems.

Security & Safety

Interested in the convergence of safety and security for cyber physical systems as a driver for system survivability and resiliency.

Rust Programming Language

Leveraging Rust for its performance and safety in system-level programming, exploring its applications in secure software development.

Model Based Systems Engineering

Actively engaged in MBSE, focusing on its integration with contemporary engineering practices to improve system design and lifecycle management. Keen interest in leveraging MBSE to perform security analyses, capture traceability, and derive security measures.