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*

- Performing applied research on the safety, security, and trustworthiness of Artificial Intelligence (AI) and autonomous capabilities.

Supernal — **July 2022 – Present**
Platform Security Engineering Lead — *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 (TARA).
- Performing systems engineering activities, following ISO 15288 and SAE ARP 4754B, including requirement development, architecture design, and V&V while coordinating performance specifications and design reviews.
- 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 Joint Strike Fighter (JSF) Joint Program Office (JPO) — **October 2021 – July 2022**
Principal Cyber Architect — *Fort Worth, TX*

- Cyber Architect (SETA) for the F-35 JSF Joint Program Office's Cyber Directorate, led the development of cyber capabilities for the F-35 Air Vehicle and collaborated with international partners on system security and mission assurance.
- Revamped the Systems Requirements Document (SRD) for cyber resiliency and survivability. Authored Statements of Work (SOWs) integrating cybersecurity engineering, software assurance, and supply chain risk management, enhancing the F-35's security posture.

Lockheed Martin — **April 2019 – 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 Technology Refresh (TR-3) and associated capabilities.
- Developed Basis of Estimates (BOEs) to execute NIST 800-53 Risk Management Framework and other activities for the Air Vehicle, its capabilities, and the ground systems (ALIS, JRE, etc.) achieving Authority to Operate (ATOs). Developed associated CDRL deliverables.
- Led design activities following DoDI 5200.39 intended to deter and delay exploitation of critical technologies and Critical Program Information (CPI) 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*

- Lead researcher performing cyber threat modeling, vulnerability discovery, mitigation, and risk reduction for complex systems.

Massachusetts Institute of Technology Lincoln Laboratory — **January 2015 – June 2018**
Staff, Secure & Resilient Technologies — *Lexington, MA*

- Led cyber resiliency and survivability of weapon systems (NDAA FY16 Sec. 1647 and FY17 Sec. 1650) focusing on the strategic implementation and assessment of cybersecurity designs in emerging military technologies.
- Collaborated with program offices and other research institutions on advanced methodologies, such as Cyber Mission Thread Analysis and Mission-Based Cyber Risk Assessment, while also conducting safety-centric cybersecurity analyses for key defense projects using the techniques STAMP and STPA.
- Founded the Industrial Control System Cybersecurity Laboratory (ICSCL) driving research into embedded system cybersecurity and contributing to the development of secure designs for Tactical Microgrids and other critical infrastructure applications.

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

- Cybersecurity Lead applying NIST 800-53 and NIST 800-82 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 Cybersecurity and Infrastructure Security Agency (CISA) performing analyses of Critical Infrastructure and Key Resources (CIKR) for systemic cyber vulnerabilities; collaborated closely with Information Sharing and Analysis Centers (ISACs).

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*

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 & OOSEM

PROJECTS

Secure Vehicle Development	This project bridges cybersecurity for aeronautics, automotive, and robotics - evaluating the regulatory environments, engineering processes, and means of compliance across industries.
Trustworthy and Resilient Autonomy	This research and development project develops approaches to implement trustworthy and resilient autonomous capabilities. This includes Multi-Monitor Run-time Assurance (MM-RTA) (ASTM F3269-21) and integration of Systems Theoretic Process Analysis (STPA).

ORGANIZATIONS

APF	Association of Professional Futurists	Friend of Foresight
INCOSE	International Council on Systems Engineering	Member
RTCA	Radio Technical Commission for Aeronautics	SC-216, Aeronautical Systems Security
USMC	United States Marine Corps	Cyber Auxiliary Volunteer