

# Brandyn Schult

[brandyn@thaliient.ai](mailto:brandyn@thaliient.ai) ❖ Irvine, CA ❖ (949) 490-0614

## SECURITY CLEARANCE

Top Secret, SCI Eligible

U.S. Department of Defense

## WORK EXPERIENCE

### Thalient Cybernetics

*Co-Founder*

**January 2023 – Present**

*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

*Lead Platform Security Engineer*

**July 2022 – Present**

*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

*Principal Security Architect*

**October 2021 – July 2022**

*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

*Manager, Cyber Security Engineering*

**July 2018 – October 2021**

*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

*Senior Security Researcher*

**July 2018 – March 2019**

*Cambridge, MA*

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

### Massachusetts Institute of Technology Lincoln Laboratory

*Associate Staff*

**January 2015 – June 2018**

*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

*Lead Cyber Security Engineer*

**June 2014 – December 2014**

*McLean, VA*

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

### Department of Homeland Security

*Cyber Security Engineer*

**May 2013 – September 2013**

*Arlington, VA*

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

## EDUCATION

### Air Force Institute of Technology

*Systems Engineering, Graduate Certificate*

**September 2022**

*Wright-Patterson Air Force Base*

### University of Maryland Baltimore County

*Cyber Security, M.S.*

**December 2013**

*Baltimore, MD*

### College of the Atlantic

*Human Ecology, B.A.*

**January 2010**

*Bar Harbor, ME*

## CERTIFICATIONS

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

## TRAINING

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

## PRESENTATIONS

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

## ORGANIZATIONS

<b>IEEE</b>	Institute of Electrical and Electronics Engineers	Former Member
<b>INCOSE</b>	International Council on Systems Engineering	Member
<b>ISO</b>	International Organization for Standardization	Member
<b>RTCA</b>	Radio Technical Commission for Aeronautics	SC-216, Aeronautical Systems Security
<b>USMC</b>	United States Marine Corps	Cyber Auxiliary Volunteer

## INTERESTS

### Cybernetics & Artificial Intelligence

Passionate about exploring the intersection of cybernetics and AI (see personal website <https://thaliient.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.