Brandyn Schult

bgschult@gmail.com Irvine, CA (207) 610-3272

SECURITY CLEARANCE

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

WORK EXPERIENCE

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

- Leading airworthiness security efforts (RTCA DO-326A, DO-355A, DO-356A, Part-IS) for an autonomous eVTOL aircraft by conducting risk assessments, developing security requirements, and integrating security measures into the design and development process.
- Conducting Threat Assessment and Remediation Analyses (TARA) using Isograph AttackTree, leveraging inputs from MITRE ATT&CK, EMB3D, D3FEND, CAPEC, CWE, CVE, and CISA's Known Exploited Vulnerabilities.
- Performing systems engineering per ISO 15288 and SAE ARP 4754B, utilizing MBSE for use cases, requirements, and architecture modeling with 3DExperience, Cameo Systems Modeler, Teamwork Cloud, and DOORS Next Generation.

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

- Spearheaded the development of cyber capabilities for the F-35 JSF Joint Program Office's Cyber Directorate, identifying warfighter needs, gaining stakeholder support, and shepherding conceptual designs into a program of record.
- Developed Statements of Work (SOWs) for MBCRA, SBOM, C-SCRM, NIST CSF/RMF, CPI, and SSE lines of effort. Coordinated across stakeholders and product teams on system security and software assurance for the F-35 JSF program.

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

- Managed cyber resiliency and survivability initiatives for the F-35 Joint Strike Fighter (JSF) and Advanced Development Programs (ADP).
- Evaluated air vehicle architecture and capabilities for security risks, performing assessments of software builds to ensure adherence to secure coding practices (C/C++) through SAST/DAST/SCA, vulnerability assessments, and code reviews.
- Led the development and submission of Basis of Estimates (BOEs) and Requirements Work Packages (RWPs), ensuring compliance with SOW requirements, accurate cost estimation, effective resource allocation, and detailed task planning for government contracts.
- Managed the development, submission, and tracking of Contract Data Requirements Lists (CDRLs) for government contracts, ensuring timely delivery and compliance with all contractual and regulatory requirements.

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

- Instructed reverse engineering, threat modeling, and anti-tamper techniques for use in Cyber Network Operations (CNO).

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

- Developed architectures and technologies to ensure the security, resiliency, and survivability of mission-critical cyber-physical systems for the Department of Defense.
- Led cybersecurity vulnerability assessments for the USAF CROWS office, focusing on both legacy and new major weapons systems, identifying critical risks and developing strategies to mitigate potential cyber threats (NDAA FY16 Section 1647).
- Applied advanced methods for cybersecurity analysis, including DREAD, PASTA, STRIDE, Cyber Mission Thread Analysis (CMTA), Mission-Based Cyber Risk Assessments (MBCRA), and Systems Theoretic Process Analysis for Security (STPA-Sec)

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

- Led the implementation of the Risk Management Framework (NIST 800-53 and NIST 800-82) for Pentagon industrial control systems (ICS), power facilities, and Chemical, Biological, Nuclear, and Explosive (CBRNE) sensors.

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

- Developed a Geographic Information System (GIS) Common Operating Picture (COP) combining real-time cybersecurity threat and vulnerability data with open-source intelligence for DHS Cybersecurity & Infrastructure Security Agency (CISA)

EDUCATION

Air Force Institute of Technology — **September 2022**
Systems Engineering, Post-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	ISC2	449871
ASEP	Associate Systems Engineering Professional	INCOSE	289361
OCSMP	OMG-Certified SysML Professional, Model User	OMG	506097

TRAINING

Advanced Security	Hardware Hacking and Reverse-Engineering
Advanced Security	Radio Frequencies (RF) and Software-Defined Radios (SDR) Hacking
KU Jayhawk	Aircraft Certification and Airworthiness Approvals
KU Jayhawk	Fundamental Avionics
KU Jayhawk	System Safety Assessment for Commercial Aircraft
RTCA	Software Considerations in Airborne Systems
RTCA	Airworthiness Security
Delligatti Associates	OCSMP Accelerator Systems Modeling Language (SysML)
Delligatti Associates	OOSEM Accelerator MBSE Methodology

PRESENTATIONS

IEEE 2022	Trustworthy Autonomy in Advanced Air Mobility
IEEE 2023	RTCA DO-326A Aircraft Security Risk Assessments leveraging MBSE and SysML

ORGANIZATIONS

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

PROJECTS

Artificial Intelligence

- Passionate about exploring the intersection of cybernetics and Artificial Intelligence (AI). Exploring effective ways to leverage Generative AI and Large Language Models (LLMs) as a force multiplier in systems and security engineering.
- Deeply interested in AI risks and trustworthiness, focusing on ensuring validity, reliability, safety, security, resilience, and trustworthy AI through rigorous risk assessments, ethical considerations, and the implementation of robust validation frameworks.

Cybersecurity Integration

- Passionate about making sense of the many disparate sources of security information, including security frameworks (NIST 800-53, ISO 27000, ISO 27001, NIST 800-171, NIST 800-160v1, NIST 800-160v2), threat information (MITRE ATT&CK, D3FEND, EMB3D), weaknesses (CWEs), and vulnerabilities (CVEs, CISA KEV).
- Developed an Airtable interactive relational database that ties these sources together, enabling comprehensive analysis and improved decision-making in security engineering.

Model Based Systems Engineering (MBSE)

- Actively engaged in MBSE, focusing on integrating it with contemporary engineering practices to enhance system design and lifecycle management. Keen interest in leveraging MBSE for performing security analyses, capturing traceability, and deriving robust security measures to ensure comprehensive system protection.