Anthony Russo, CISSP

(512) 626-5816 | anthony.russo.7@outlook.com | linkedin.com/in/atrusso7/ | anthony-russo.com | github.com/atrusso7

CYBER SECURITY ANALYST | APPLICATION DEVELOPER | PROGRAMMER

A talented IT Professional with strong expertise in cybersecurity analysis, network monitoring, and malware. Skilled at using digital forensic tools to create reports and present them to superiors. Adept at working with staff at all levels.

Core Proficiencies

SIEM	**IDS**	**OS**	**Red Team**
Splunk/Elastic	Snort/Suricata/Bro	RHEL/SIFT/Kali/SO/Windows	Metasploit/Burp Suite
Dev	**ML**	**Tools**	**Forensics**
C#/Python/.NET/SQL/Azure	SciKit-learn/TensorFlow	Wireshark/TCPDump/Sysinternals	Cuckoo/Volatility

Certifications: CISSP, CSAP, CySA+, Security+, Network+, and MTA: Software Development Fundamentals

Clearance: Active Secret

Professional Experience

Microsoft Software Systems Academy, JBSA Randolph, San Antonio, TX Jan 2020 - Present

Student

Focus and study in Cloud Application Development, learning to design, write, build and support applications and programs. Gained fundamental skills in Azure, C#, SQL, CSS, and HTML. Learn conceptual frameworks for Web Applications development, ASP.NET MVC, and Azure Application Development

- Developed and implemented web applications that meet a set of functional requirements, user interface requirements, and address business models
- Created modern web apps and services on the MS web technologies stack using ASP.NET
- Designed Azure solutions – configured, managed, monitored and scaled ARM VMs and storage

US Air Force, Aviano Air Base, Italy May 2016 - Present

Cyber Security Analyst

Lead threat hunt operations team, handling **network monitoring**, **incident response**, and **digital forensics**. A crucial member in establishing one of Europe's first cyber defense teams.

- Configured SIEM (ELK) through sensor placement and used Elasticsearch to develop Kibana visualizations
- Performed network enumeration to eliminate false positive/negative alerts and craft custom IDS signatures
- Provided cradle-to-grave incident response on-base malware incidents from preparation to post-incident activities
- Investigated incidents with digital forensic tools to generate reports and presented them concisely to superiors
- Managed AES encrypted $18.2 million Enterprise Land Mobile Radio network comprised of 3,000 users

Additional Experience: 5+ years customer service, 4+ years network administration, and 3+ years web development

Education

Embry-Riddle Aeronautical University

Bachelor of Science in Interdisciplinary Studies, Minor in Communications

Community College of the Air Force

Associates of Arts & Sciences in Electronics Systems Technology

Advanced Training

- SEC 503, Intrusion Detection In-Depth, SANS Institute, London, UK
- SEC 511, Continuous Monitoring, SANS Institute, Prague, CZ
- Functional Mission Analysis, Air Force Cyber College, Ramstein Air Base, DE
- Tacet Venari, DoD Cyberwarfare Exercise, Ramstein Air Base, DE
- Airmen Leadership School, Aviano AB, IT