Anthony Russo, CISSP

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

A talented IT Professional with a unique blend of expertise in cybersecurity analysis, technical troubleshooting, leadership, and customer service. Skilled at mastering technology stacks in order to contribute to operations and support. A recognized innovator who is adaptable and dependable. Adept at working with staff at all levels.

Core Proficiencies

Expert: Network analysis, incident response, threat hunting, leadership, teamwork, customer service, problem solving, innovation, and collaboration

Experienced: Digital forensics, Splunk, Elastic Stack, McAffee, Azure, O365, penetration testing, IDS, IPS, Kali, and compliance

Competent: C#, .NET, Python, SQL, AWS, Volatility, Burp Suite, and Metasploit

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

Clearance: Active Secret

Professional Experience

Texas Workforce Commission, Austin, TX Jun 2020 - Present

Cyber Security Analyst

Security Monitoring and Incident Response Team member charged with identification, protection, detection, response, and recovery from threats and incidents.

- Investigate and remediate 400 monthly phishing attempts using Splunk, O365, Azure ATP, and other forensic tools
- Proactively threat hunt on a network of 5000+ assets by leveraging IPS, SIEM, Endpoint, and Cloud solutions
- Respond to 500 monthly trouble tickets – diagnose, troubleshoot, and remediate technical issues related to proxy, phishing, and security concerns
- Administrate enterprise Splunk log aggregation server that ingests 5 million daily events from 3 heavy forwarders

Microsoft Software Systems Academy, JBSA Randolph, San Antonio, TX Jan 2020 – May 2020

Apprentice

Focused and studied in Cloud Application Development, learned to design, write, build, and support applications and programs. Gained fundamental skills in Azure, C#, SQL, CSS, and HTML. Learned 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
- Facilitated team project – identified a need, distributed workload, collaborated, and produced cloud application

US Air Force, Aviano Air Base, Italy May 2016 – May 2020

Cyber Security Analyst

Led threat hunt operations team, handled 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
- Directed Security Fundamentals course that increased CompTIA Security+ pass rate from 33% to 87%
- Onboarded 15 new Tier I/II analysts by providing extensive tactics training and continued mentorship
- 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

American Home & Commercial Services, Liberty Hill, TX Jan 2010 – May 2016

Network Admin/Web Developer

Managed and maintained small-business network of +75 devices. Designed and developed company website utilizing on-premise services.

- Incorporated Identity Access Management (IAM) system of 20 users to ensure robust security posture
- Redesigned company website that boosted daily views 50%, sales leads 15%, and 5% annual revenue
- System remained available 99.99% during 5 years of oversight and never reported a security incident

Education

Texas State University *(In Progress)*

Master of Business Administration, Concentration in Computer Information Systems

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

- AZ-500 Microsoft Azure Security Engineer, NetCom Learning, Online
- SEC 503, Intrusion Detection In-Depth, SANS Institute, London, UK
- SEC 511, Continuous Monitoring, SANS Institute, Prague, CZ
- Tacet Venari, DoD Cyberwarfare Exercise, Ramstein Air Base, DE
- Airmen Leadership School, Aviano AB, IT
- Air Force Survival School, Fairchild AFB, WA