

# Anthony Russo, CISSP

(512) 626-5816 | [anthony.russo.7@outlook.com](mailto:anthony.russo.7@outlook.com) | [linkedin.com/in/atrusso7/](https://www.linkedin.com/in/atrusso7/) | [anthony-russo.com](http://anthony-russo.com)

## CERTIFICATIONS

---

CISSP | Active Secret Security Clearance | AWS: Cloud Practitioner | Rapid7: Advanced Vulnerability Manager | Rapid7: InsightIDR Specialist | Rapid7: InsightVM Administrator | CompTIA: Security Analytics Professional (CSAP) | CompTIA: Cybersecurity Analyst (CySA+) | CompTIA: Security+ | CompTIA: Network+ | MTA: Software Development Fundamentals

## PROFESSIONAL EXPERIENCE

---

### Technical Account Engineer

Aug 2020 – Present

*Rapid7 | Austin, TX*

Premium Support team member responsible for rapid response, account management, and technical advising on Rapid7 product offerings.

- Conduct **in-depth analysis** including but not limited to reviewing code for potential defects and partners with the Development team when necessary
- Helping build a brand-new support service from ground up including onboarding procedures, communication strategies, and team workflow
- Develop rapport with customers by providing exceptional **customer service** through communication, solutions, and advocacy
- Oversee and consult on accounts for Rapid7's Premium Support customers ensuring the delivery of positive experience, **technical support**, and guidance

### Cyber Security Analyst

Jun 2020 – Aug 2020

*Texas Workforce Commission | Austin, TX*

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

- Investigated and remediated 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
- Responded to 500 monthly trouble tickets – diagnosed, troubleshoot, and remediated technical issues related to proxy, phishing, and security concerns

### Cloud Application Development Apprentice

Jan 2020 – May 2020

*Microsoft Software Systems Academy | JBSA Randolph, TX*

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

## Cyber Security Analyst

May 2016 – May 2020

*US Air Force | Aviano Air Base, Italy*

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
- Crafted custom **Python** scripts that incorporated **machine learning** to identify patterns within netflow, pcap, and end-user behavior
- Onboarded 15 new Tier I/II analysts by providing extensive tactics training and continued mentorship
- **Analyzed malicious network traffic** with tools like **Wireshark** to storyboard attack vectors and impact
- 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

## Network Admin/Web Developer

Jan 2010 – May 2016

*American Home & Commercial Services | Liberty Hill, TX*

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 (*GPA 3.6*)

### Community College of the Air Force

Associates of Arts & Sciences in Electronics Systems Technology (*GPA 4.0*)

## 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