Ava E Baratz
ava.baratz1@gmail.com
About Me | ava-baratz

OBJECTIVE

Motivated and detail-oriented Cybersecurity professional with a strong academic foundation and extensive experience in compliance, risk management, and incident response. Equipped with industry-recognized certifications, including CASP+, CySA+, and AWS Certified Cloud Practitioner, I aim to enhance organizational security posture and contribute to achieving strategic cybersecurity objectives in dynamic, collaborative environments.

Education

Old Dominion University, Norfolk Va. Bachelor of Science in Cybersecurity **Minor:** Risk Management and Insurance **Cumulative GPA**: 3.92

Certifications:

CompTIA Security + Certification - November 2023
CompTIA CySA+ Cybersecurity Analyst Certification - June 2024
AWS Certified Cloud Practitioner Certification - February 2024
CompTIA CASP+ Certified Advanced Security Practitioner - November 2024

Training:

Tenable - March 2024
Red Canary - March 2024
Carbon Black - March 2024
CMMC - August 2024
eMASS - September 2024
Certified Incident Handler (ECIH) v2 - March 2024
Amazon Web Services - February 2024
Ethical Hacking - August 2023
Python - January 2023
Linux - August 2022

Professional Experience

QinetiQ Inc. - McLean, Virginia
Cybersecurity Analyst
June 2023 - Present

- Ongoing compliance support for the US Customs and Border Protection’s Tethered Aerostat Radar System (TARS) ISSO.

- Reviewed Nessus scans weekly and submitted to the system administrators for remediation
- Executed tasks associated with achieving and maintaining an Approval-to-Operate (ATO) within the Risk Management Framework (RMF) using eMASS IA Manager tool.
- Developed, executed, and documented security risk assessment following NIST 800-53, control requirements, ran SCAP tools and assisted implementing Security Technical Implementation Guidelines (STIGs).
- Conducted a pre-assessment and evaluation of security controls and documented security control compliance status.
- Performed technical coordination with network engineers and system administrators involved with implementing and maintaining controls, the system security plan, contingency plan, and other documents required for an information systems authorization package.
- Lead CMMC Level 2 assessment preparation to gather appropriate documentation among all cyber and information technology members.
- Lead ISO 27001 certification preparation.
- Developed and maintained a continuous monitoring plan for ongoing compliance with NIST 800-171 controls.
- Performed continuous monitoring and incident response for end-point security stack tools, including Sentinel, Carbon Black, Red Canary, Trellix, and Microsoft Defender.
- Responsible for developing and reviewing policies, plans, and other security documentation.
- Patched Windows 11 workstations using WSUS.
- Used SolarWinds to review node availability, and network latency, analyzed and created custom reports for management.
- Developed information technology and cybersecurity policies in compliance with the NIST SP 800- 171 Revision 3 framework.
- Developed an enterprise-wide System Security Plan (SSP).
- Increased Microsoft compliance manager score from 35% to 86% in one week.
- Developed and implemented cybersecurity compliance metrics.
- Created an initiative for improving organizational phishing compliance scores.