Benjamin Justice

Senior Cybersecurity Analyst

Location: Baltimore, MD
Phone: (443) 796-6424
Email: benjustice359@gmail.com

PROFESSIONAL EXPERIENCE

Cyber National Mission Force, 21 Cyber Protection Team, Ft. Meade, Maryland – Crew Lead

October 2023 - Present

- As Joint Mission Element 1 Crew Lead at 21 Cyber Protection Team (CPT), advised and led National leaders, Foreign Leaders, Naval Officers, and Non-Commissioned officers in response to cyber incidents affecting The United States, U.S. Allies, and critical military networks.
- Led the support and systems analysis of forward deployed cyber hunts on compromised networks.

Navy Cyber Defense Operations Command, Suffolk, Virginia - *SOC Manager*

December 2022 - October 2023

- As Senior SOC Manager, advised and led Naval Officers/Non-Commissioned Officers (NCO) essential defensive cyber operations in support of 3,800+ ashore and afloat Naval Units in a 24/7 operational environment.
- Directed the analysis of cyber events/incidents for 30+ personnel across six teams, mitigating malicious cyber incidents for global Naval operations.
- Oversaw and directed the analysis of SIEM (Splunk Enterprise Security/Azure Sentinel) and IPS/IDS (Cisco SourceFire/McAfee Intrushield) alerts in near-real time, ensuring quick and accurate cyber event/incident reporting and response.
- Managed 2,300+ Cyber Incident Investigations across seven Naval Operational Enterprise Networks, resulting in the mitigation of 300+ malicious and unauthorized cyber incidents.
- Planned, executed, and evaluated routine and emergency operations; led fleet-wide and joint-DOD exercises for cyber-readiness efforts.

Navy Cyber Defense Operations Command, Suffolk, Virginia - *SOC SIEM Engineer*

June 2022 - PRESENT

- As a Splunk and Azure Sentinel operational expert for the Navy, Ingested Office 365 Federal: Endpoints, Identity; Cisco Intrusion Prevention System (Snort) alert logs, and Zeek (BRO) Intrusion Defense System Logs into SIEM tools.
- Performed investigations into organizational inefficiencies and provided recommendations to automate or leverage existing tools, leading to automating all Tier 1 positions on the Navy's 24/7 watch floor. Reducing the incident response time by 92%.
- Create event triage logic to filter 3.1 billion events into 67 quality

CERTIFICATIONS

CompTIA CySA+

CompTIA Linux+

CompTIA Security+

CompTIA A+

Certified Ethical Hacker (CEH)

EDUCATION

University of Maryland Global Campus, Adelphi, MD Bachelor of Science - *Cybersecurity Management and Policy*

September 2021 - December 2023

GPA: 4.0

University of Maryland Global Campus, Adelphi, MD Associate of Arts - General Studies

September 2021 - August 2023

GPA: 4.0

incidents a day. Develop industry-standard training on the management and use of SIEM and SOAR solutions in an enterprise environment.

Navy Cyber Defense Operations Command, Suffolk, Virginia - *SOC Tier - 2 Lead Analyst / Training Lead Instructor*

December 2021 - December 2022

- Provided Tier 2 analysis to SOC analysts mitigating potential intrusions and other malicious activity, to include APT related threats, in support of the Navy's premier CSSP.
- Performed Quality Control for Network Forensics team reports, ensuring potential IOCs were discovered in network traffic and all proper analysis pipelines were leveraged during investigations.
- Spearheaded operational overhaul for SOC Network Forensics training pipeline, standardizing and implementing new TTPs improving training methods and analytical processes.
- Revised and created 20+ Standard Operating Procedures (SOP) in adherence with industry standards (i.e., NIST, ISO 27001, COBIT) and best practices.
- Provided leadership and technical training for personnel in three SOC work roles, conducting qualification boards supporting SOC manning.

Navy Cyber Defense Operations Command, Suffolk, Virginia - *SOC Tier - 1 Lead Analyst*

October 2020 - December 2021

- Led 3 teams consisting of 15 analysts to perform advanced security detection and threat analysis via SEIM/IPS platforms (Splunk Enterprise Security/Cisco Sourcefire) for complex cyber intrusion events/incidents, providing actionable intelligence to affected units and stakeholders and 100 percent mitigation of discovered malicious activity.
- Provided technical leadership support and remedial recommendations throughout the life cycle of incidents through authoring in-depth reports documenting all activity that occurred during investigations.
- Collaborated with cross-functional teams in threat hunting and intelligence to identify and mitigate emerging threats and APT-related activity across 3,800+ Naval Units.
- Monitored and conducted technical-health assessment of 150+ global IPS/IDS sensors in support of defensive cyberspace operations.
- Technical signature analysis drove network signature modification of false-positive alerts, ensuring accurate detection and response to cybersecurity events.
- Directly collaborated with Malware Analysis, Incident Handling and Response, and SIEM divisions in response to timely discovery, response, and mitigation of cyber events and incidents.

SKILLS

Network Forensics

Host Forensics

SIEM (Splunk, Azure, Kibana)

Data Analysis/Visualization

SOC Management

Cybersecurity Management

Threat Hunting

Threat Analysis

Defensive Cyberspace Operations

Python

Powershell

Windows

OTHER NOTABLES

Active Duty U.S. Navy through March, 2028

Top Secret/SCI Security Clearance