Jonathan Gatell (954) 663-0290 | Top Secret/SCI+CI Poly | Alexandria, Virginia | gatellj@gmail.com

GIAC Certified Forensics Analyst (GCFA) | GIAC Penetration Tester (GPEN) | GIAC Certified Incident Handler (GCIH)
Comptia Cybersecurity Analyst (CYSA+)

United States Coast Guard

Senior Windows Analyst, Cyber Protection Team, CGCyber | *Washington, D.C.* | 05/*2020 – Present*

Deployable member of threat hunting, incident response team, and penetration team, with a focus on Windows host forensics (DFIR). Work on call rotation to meet 24/7 deployable availability.

- Conducted threat hunting operations on critical state and unit infrastructure, analyzing 1000's of assets per engagement based on relevant threat landscape, using Carbon Black and Splunk for host analysis.
- Developed after action reports and incident reporting for leadership and partner management
- Provided recommendations in order to advance the security posture of partners during and after an incident, increasing security posture.
- Lead development of incident response network sensor monitor, collaborating with cross functional teams for to ensure standard kit deployment. Determined functional requirements while using open source and commercial tools.
- Developed standard operating procedures and runbooks for future deployment of kit. Created automated script to install different components of kit software, saving stand up time and work hours before mission engagements.
- Identified and implemented standard threat emulation techniques to test the efficacy of the sensors and rulesets on simulated customer networks, ensuring future system operate correctly

Senior Event Detection Analyst, Security Operation Center, CGCyber | *Washington D.C.* | 03/*2019 – 05/2020*

Member of watch rotation on Coast Guard Enterprise wide CSOC watch floor in addition to daily threat hunting activities.

- Conducted threat hunting operations against APT's based on threat intelligence.
- Used centralized logging before pivoting to specialized tools to parse terabytes of information. Managed alert triage queue, prioritizing serious to false positives.
- Prepared event reports with analysis methodology, root cause analysis, and results.
- Responded to event and incident escalations from security operations center watch floor.
- Used Python and Powershell to automate data sorting or enterprise-wide management of evidence and log collection, as well as phishing/spam email deletion.
- Mentored junior analysts on threat hunting methodologies as well as professional development.

Network/Systems Operation Center, Enterprise Ops, CGCyber | *Alexandria, VA* | 05/*2018 – 03/2019*

- Coordinated repair of Coast Guard wide enterprise information technology systems.
- Conducted remote monitoring on network hardware, Windows Active Directory, and Nationwide Automatic Identification System.
- Accessed CISCO routers and switches to troubleshoot the issues remotely, reducing technician workloads.

Avionics Electrical Technician, Aviation Training Center | *Mobile, AL* | *11/2014 – 05/2018*

- Maintained all electronic components of MH60-T Jayhawk, including software patching, comms/radio and automatic navigation system troubleshooting.
- Managed communication crypto keys as COMSEC manager, trained members on proper crypto handling.
- Trained junior members on hangar deck operations, aircraft inspections, and development opportunities.
- Managed the establishment of maintenance shop in forward operation location for Hurricane Harvey response.

Operating Systems, Coding Languages, and Tools: Linux (RHEL and Debian based), MacOS, Windows, Python, C, C++, Java, Bash**,** Carbon Black, Zeek, Snort, Volatility Framework, Wireshark, Splunk, Burpsuite, JIRA, BitBucket

Information Warfare Training Center | *Pensacola, FL*

Joint Cyber Analysis Course, November 2019

Florida International University | *Miami, FL*

Bachelor's Degree in Computer Science, Expected 2022

University of Central Florida | *Orlando, FL*

Associate' of Arts, Awarded 2021