Available August 2021

Jonathan Gatell

Alexandria, Virginia | (954) 663-0290 | 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 (2013-Present)

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

Deployable member of threat hunting, penetration testing, and incident response team, focused in Windows host forensics (DFIR), but working in Linux and network environments.

- Conducted threat hunting operations on critical state and unit infrastructure.
- Provided recommendations in order to advance the security posture of partners during and after an incident.
- Developed incident response deployment kit. Determined functional requirements while using open source and commercial tools.
- Wrote and edited Snort and YARA rules provided by intelligence sources. Tuned relevant rules based on mission requirements.
- Developed standard operating procedures and runbooks for future deployment of kit.
- Used threat emulation techniques to test the efficacy of the sensors and rulesets on simulated customer networks.

Senior Event Detection Analyst, Security Operation Center, CGCyber | *Washington D.C.* | *2019 – 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 gigabytes of information and focus the search down to relevant data.
- Managed alert triage queue, prioritizing serious to false positives,
- 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 email deletion.
- Mentored junior analysts on threat hunting methodologies as well as Coast Guard skills.

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

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

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

- Maintained all electronic components of MH60-T Jayhawk, including software patching, comms/radio and automatic navigation system troubleshooting.

Programming languages: Python, C, C++, Java, Bash

Security Tools: Carbon Black, Zeek, Snort, Volatility Framework, Wireshark, Splunk, Burpsuite, RITA

Operating Systems: Linux (RHEL and Debian based), MacOS, Windows

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