THOMAS GORMAN

gormantg@gmail.com | github.com/Tsora-Pop

Summary:

I am a cyber security professional with 4.5 years of active “Blue Team” security experience and 8 years of threat analysis experience and 12 years of technical work. I have worked with a Security Operations Center, an Incident Response Team, and with a Managed Detection and Response team. I have undertaken various cyber security courses to broaden my perspective.

Certifications & Courses:

- PWK(PEN-200) | In Progress
- SANS SEC401 | Certification: GSEC
- SANS SEC504 | Certification: GCIH
- SANS SEC542 | Not Certified
- SANS SEC511| Certification: GMON
- ISACA CSX-P Course
- MNEX WireShark and Network Analysis Training
- Applied Network Defense: Intrusion Detection and Prevention with Suricata

Skills:

SIEM/SOAR	ArcSight, Sentinel, Splunk
Endpoint	Microsoft Defender for Endpoint(EDR), Tanium, McAfee EPO, Sophos Managed Threat Response, OSQUERY
Network	PFSense, Unifi, NetWitness, Wireshark, Suricata, Tipping Point, Palo Alto
Cloud	Sophos Central, Azure Portal (Manual Hunting), AWS Route 53 and Lightsail
Ticketing/ Documentation	JIRA, ServiceNow, Confluence
Languages	Query: KQL, SQL Markup: HTML Scripting: Powershell, Bash Compiled: C#, Learning Rust
Projects	Contributor to Atomic Red Team
Penetration Testing	Burp Suite, NMAP, Enumeration
Past/Other	Regex, Elastic, VMWare ESXi, Python, PostgreSQL, FTK Imager, MS Visio, MS Project, Web Design, Business Management on Google Maps, Slack RSS Feed Channel, Archer, Teams

Employment History:

Threat Analyst II
Sophos: September 2020 – February 2021 | Carmel, IN
I provided monitoring, detection, and response services and proactively hunted for threats within customer environments while employed with Sophos's Managed Threat Response team. I utilized MTR and Sophos Central to facilitate investigation, identification, and neutralization of cyber threats. Within the first few weeks of starting, I vastly improved the Health Check process and reduced the time to completion. I provided proactive recommendations to customers to improve their security posture and minimize risk.

Senior Intrusion Analyst
Walmart: February 2020 – September 2020 | Bentonville, AR
I created detections for a popular Endpoint, Detection, and Response product that align with the MITRE ATT&CK Framework, assisted the Microsoft Detection and Response Team while hunting, stood in as a backup Shift Lead, contributed to Atomic Red Team, and reviewed hunting dashboards for possible escalations. As I identified vulnerabilities, I reported them to appropriate teams with the impact it causes and recommended possible remediation measures.

Intrusion Analyst III
Walmart: January 2018 – January 2020 | Bentonville, AR
While employed with Walmart's Security Operations Center, I worked to ensure the safety of not only Walmart but every merger and acquisition. Through the use of SIEM, several signature detection products, endpoint protection products, and various other tools, I analyzed and responded to network activity that could pose a threat.

Incident Response Intern
Virginia Information Technologies Agency: May 2016 – August 2016, December 2016 – January 2017, May 2017 – Aug 2017 | Chester, VA
I served Virginia as an Incident Response Specialist Intern at VITA. Here I gained experience with virtual machines, NFS, a SIEM, various Linux distributions, and Honeypots. I forwarded log data for threat correlation and visual representation. I gained experience maintaining several different databases.
I upgraded the forensics lab and assisted with installation and configuration of new servers and diagnostic equipment. I also migrated a physical CentOS server to a different distribution. I coordinated with the SOC while upgrading Google Maps JavaScript API in use on a web application that Geolocated IP addresses that displayed on a SIEM dashboard.

Network Technician III
Virginia Commonwealth University: January 2017 – May 2017| Richmond, VA
I demonstrated to new hires the process of surplus. I would arrive to work a few minutes early to look at the scheduled jobs for the day and decide on a plan of action. I created new workbench instructions for new hires that provide a step-by-step process of installing our baseline image on Dell workstations.

Network Technician I
Virginia Commonwealth University*:* April 2014 – December 2016 | Richmond, VA
As a Network Technician with VCU, I provided level one support to any calls made regarding computers, printers, and network issues in the School of Humanities and Sciences. I collaborated with various departments during the setup of over 16 computer labs. I solved driver and BIOS issues on malfunctioning machines. I communicated with end users while remote support troubleshooting. I addressed Blue Screen of Death issues by recovering data and providing a new machine or hard drive, as well as informing users on how to use Google Drive. Operating systems typically used are Windows 7, XP, and various Mac Operating Systems.

Sonar Technician Third Class
United States Navy
Military Rank: E-4 | **Clearance:** Secret expired January 2016
Active Duty: January 2010 – January 2014 | Norfolk, VA
Individual Ready Reserve: January 2014 – April 2017

Education:

Bachelor of Science in Information Systems, December 2017
Virginia Commonwealth University, Richmond, VA, GPA: 3.204

Achievements/Accomplishments/Awards

SANS CyberStart Participant, 2017
Finished in the top 20%

Navy Achievement Medal, 2013

Enlisted Surface Warfare Specialist, 2011