Thomas Gorman

Durham, NC | Open to work in RTP, NC area or remote
Mobile: 804.837.3927 | gormantg@gmail.com | github.com/Tsora-Pop | tsora-pop.github.io

Summary:

I am a cyber security professional in the field since May 2016 with about 12 years of technical experience. I have undertaken various cyber security courses to broaden my perspective and to understand attack vectors. I am looking for a role where I can continue leading in the defensive cyber security field and work with a proactive team who's passion matches my enthusiasm.

Certifications & Courses:

- Applied Network Defense: Investigation Theory | 2021
- Fortinet NSE 1-3 | 2021
- PWK(PEN-200) Course | 2021
- SANS SEC511| Certification: GMON | 2020
- Applied Network Defense:
  Intrusion Detection and Prevention with Suricata | 2020
- ISACA CSX-P Course | 2018
- MNEX WireShark and Network Analysis Training | 2018
- SANS SEC542 Course | 2017
- SANS SEC401 | Certification: GSEC | 2017
- SANS SEC504 | Certification: GCIH | 2017

Skills and Tools:

SIEM/SOAR	Cybraics, Elastic, FortiSIEM, ArcSight, Sentinel, Splunk
Endpoint	SentinelOne, Cylance, 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	Zendesk, Footprints, JIRA, ServiceNow, Confluence
Languages	Query: KQL, SQL Markup: HTML Scripting: Powershell, Bash
Projects	Past contributor to Atomic Red Team
Automation	Reduced Health Check Time, Customer Health Monitoring Script
Other	Regex, VMWare ESXi, FTK Imager, MS Visio, MS Project, Web Design, Business Management on Google Maps, RSS Feed Channel, Archer, Teams

Employment History:

Security Operations Center Manager - United States

SilverSky: January 2022 - Current | Morrisville, NC

As SilverSky's US based SOC manager, I direct and oversee the daily activities of our SOC analysts in the US based SOC. I also support our international teams in Belfast, Northern Ireland and Manila, Philippines by coordinating our SOC members to provide better monitoring coverage. In addition to continuing to have all responsibilities from SOC Team Lead, I also onboard new customers by configuring collectors or API credentials in our SIEM, verify detection coverages for both new and existing customers, and make hardening recommendations for new customers to better protect their environment and reduce the incident volume for analysts.

Security Operations Center Team Lead

SilverSky: July 2021 - January 2022 | Morrisville, NC

As a SOC Team Lead, I am the primary escalation point for all cases coming from SOC analysts, tune existing detections, identify root cause of incidents, demo SIEM and other products from vendors, complete Incident Reports, and train analysts. I am also acting manager for our US SOC. Some of my primary responsibilities in this role include interacting with customers and partners for periodic site reviews, establishing guidelines for documentation, and assisting other division SOCs as needed. I navigate high tension meetings carefully to maintain progressive discussions. I conduct interviews for SOC analyst openings, take measures to raise employee morale and retention, as well as process resignations . When a critical vulnerability in a customer's environment is discovered, I will notify them in a timely and clear manner and provide mitigation recommendations.

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 from what could sometimes take over 45 minutes to about 10 minutes. 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 – February 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. After taking initial containment procedures, I would escalate the case to our Incident Response team as needed. I operated as a backup night shift lead starting in August 2018.

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 instructed new hires in the process of surplus. I would arrive at 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 – January 2017 | 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.

Education:

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

Organizations:

Association of Information Technology Professionals at Virginia Commonwealth University : March 2014 to December 2017
I served on the board for the Association of Information Technology Professionals at VCU as a Professional Development Specialist to promote career growth amongst our 100 person membership body. Responsibilities included reviewing resumes, LinkedIn creation workshops, and promoting career fairs. I represented AITP@VCU at recruiting events to invite individuals to apply for membership.

Military Service:

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

Achievements/Accomplishments/Awards

SANS CyberStart Participant, 2017
Finished in the top 20%

Navy Achievement Medal, 2013

Enlisted Surface Warfare Specialist, 2011