David H. Rogers
(410) 430-1532 (c)
drogershh15@gmail.com

OBJECTIVE:

To work for an organization that will provide an opportunity for challenge and professional growth, and to continue my career in Cybersecurity using the skills developed from my work and education experience.

EDUCATION:

Towson University Towson, MD | 2014-2018
Bachelor of Science - Computer Science / Computer Security Track

Johns Hopkins University Baltimore, MD | 2022-2024
Master of Science - Cybersecurity

CERTIFICATIONS:

- Active Top Secret Clearance
- CompTIA CySA+
- CompTIA Security+
- AWS Solutions Architect Associate

TECHNICAL SKILLS:

System Administration: Active Directory, Group Policy, ESXi, WSUS, NetBackup

Cyber Analyst: Snort, Kibana, Azure Sentinel, tcpdump (pcap), Splunk, ACAS, HBSS

Scripting Languages: Python, PowerShell, Bash, Perl

Operating Systems: Linux (Ubuntu, CentOS, Kali, Red Hat), Windows (10,Server 2016)

Security Software: WireShark, Nmap, Metasploit, Volatility, GDB, OllyDbg, IDA

Source Control: GitLab, GitHub, Team Foundation Server

WORK EXPERIENCE:

Enlighten IT Consulting (Air Force BDP) Linthicum Heights, MD | August 2020 – Present

Senior Cybersecurity Engineer / Data Scientist

- Lead a team of 8 cybersecurity analysts and data scientists using agile methodology in hunting for malicious and unauthorized network and host based traffic
- Work closely with Air Force leadership to gather requirements for analytic improvements and cyber use cases
- Perform cyber hunting for IOCs and anomalous activity in customer data sets utilizing analytics
- Create intrusion detection rules in lucene syntax to detect malicious or anomalous activity
- Utilize the MITRE ATT&CK matrix for tracking TTPs used by APTs and other cyber threat actors
- Train users of the BDP trough bi-weekly technical presentations
- Analyze, enrich, and parse data feeds including Zeek, Palo Alto Pan-OS, Windows EVTX, AWS Cloudtrail, AWS VPCFlow, O365, Cisco Router, McAfee HBSS, Kubernetes, Netflow, AppGate, Tanium, Blue Coat Proxy, PowerShell, Sysmon, and more
- Create Python scripts utilizing regex to parse various file types including json, xml, yaml, and csv
- Create Kibana dashboards to visualize data of interest
- Propose data standardizations to aid in cross data feed queries such as MAC addresses, hostnames, domains, and users
- Map various data feeds to the Elastic Common Schema

EmeSec (Army Research Laboratory) Adelphi, MD | December 2019-August 2020

Senior Cybersecurity Analyst

- Lead a team of 4 in hunting for malicious and unauthorized network and host based traffic
- Worked closely with senior leadership to define security monitoring requirements
- Assigned duties based on monitoring requirements

Cybersecurity Analyst

- Developed and modify scripts to monitor network traffic using Bash, Perl, and Python
- Monitored intrusion detection systems using Snort and other proprietary IDS/SIEM tools
- Created Snort rules to match malware and unauthorized activity signatures from OSINT and IOC
- Analyzed anomalous network activity using the ELK stack (Elasticsearch, Logstash, Kibana), and Azure Sentinel
- Monitord Azure, AWS, o365, and ServiceNow cloud environments
- Utilized tcpdump, sed, awk, and grep for pcap analysis
- Published monthly cyber threat research to be used throughout DoD
- Created technically detailed reports based on intrusions and events

Concept Plus (Aberdeen Proving Ground) Edgewood, MD | March 2019-December 2019

Systems Engineer

- Conducted weekly ACAS scans against the network consisting of 40 servers and 15 workstations
- Maintained Active Directory by adding and removing users and computers as needed
- Maintained multiple virtual machines via VMware vSphere including taking snapshots, allocating memory as needed, and regular maintenance checks
- Implemented monthly OS patches and software patches on the servers and workstations via WSUS over remote PowerShell and SCCM maintained by the hosting site
- Performed weekly tape backup via Veritas NetBackup
- Tracked IAVAs and POA&Ms as applicable to the servers and workstations on the network
- Ensured network health by maintaining a WhatsUp server
- Tracked installed software and software versions by maintaining a TrackIt server

Software Engineer

- Developed and maintain a Java EE web application deployed on Oracle WebLogic integrated through web services with a distributed Windows .NET (C#) desktop application.
- Used Java, Oracle products, Microsoft .NET C#, Microsoft TFS, SharePoint, Crystal Reports.

AMSAA (U.S. Army) APG, MD | May 2018-August 2018

ORISE Software Engineer Internship

- Created a full stack web application using Java EE as the back end to connect to an Oracle database and XHTML, CSS, JavaScript, Prime Faces, and Java Server Faces for the front end
- Created multiple tables in the Oracle database using SQL to be referenced throughout the web application
- Hosted the application using WebLogic and source control using Microsoft TFS

ADG Creative Columbia, MD | May 2017-October 2017

Web Development Internship

- Converted a static HTML/CSS site into a WordPress framework where a content manager can edit content without seeing a line of code
- Used PHP to create an interactive job posting board that deleted cells without content and added cells with content
- Used the phpMyAdmin database for the website's content that can be changed from the WordPress admin console