

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

CERTIFICATIONS:

- Active Top Secret Clearance
- Active Public Trust Clearance
- IAT II
- CompTIA CySA+
- CompTIA Security+
- AWS Solutions Architect Associate

TECHNICAL SKILLS:

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

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

Scripting Languages: Python, PowerShell, Bash

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

Security Software: Wireshark, Nmap, Scapy

Source Control: GitLab, GitHub, Team Foundation Server

WORK EXPERIENCE:

Booz Allen Hamilton (DOL NCFMS)

Remote | March 2022 – Present

Senior Cybersecurity Engineer

- Administer, monitor, analyze, and respond to security alerts in Splunk, Security Onion, Kibana, and Symantec Endpoint Protection
- Lead vulnerability management for all NCFMS environments.
- Research vulnerability mitigation steps and work closely with the system administration team for servers including Windows, and Oracle Enterprise Linux servers, ESXi, F5 load balancers, Cisco routers & switches, and various Oracle enterprise applications
- Modify Suricata rules from Emerging Threats to limit false positives
- Implement Yara rules provided by CISA to be used in Security Onion
- Hunt for IOCs including domains, IP addresses, and hashes in Zeek and PCAP data
- Utilize tcpdump and Wireshark for analyzing PCAP data
- Conduct web application scanning utilizing Burp Suite for application releases and compliance
- Scan network assets for vulnerabilities utilizing Nessus
- Respond to CISA directives that require patching for affected network assets
- Utilize Python, PowerShell, and SQL scripts for automating patching tasks and querying user account details
- Administer access for all 100+ NCFMS users utilizing role-based access controls
- Maintain cybersecurity documentation deliverables including system access, network processes, patch management, PII data management, and change control SOPs

- Provide guidance for cybersecurity initiatives such as implementing zero trust, IPv6 transition, data encryption, FISMA assessments, and NIST SP 800-53 Rev 5 compliance

Enlighten IT Consulting (Air Force BDP)

Linthicum Heights, MD | August 2020 – March 2022

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
- Worked closely with Air Force leadership to gather requirements for analytic improvements and cyber use cases
- Performed cyber hunting for IOCs and anomalous activity in customer data sets utilizing analytics
- Created 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
- Trained up to 100 users of the BDP through live bi-weekly technical presentations
- Analyzed, enriched, and parsed 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
- Created Python scripts utilizing regex to parse various file types including json, xml, yaml, and csv
- Created Kibana dashboards to visualize data of interest
- Proposed data standardizations to aid in cross data feed queries such as MAC addresses, hostnames, domains, and users
- Mapped various data feeds to the Elastic Common Schema

EmeSec (C5ISR CSSP 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 Kibana and Azure Sentinel
- Monitored 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