TONY DURHAM

Active Public Trust Clearance

571-260-8641

dreambig.td@gmail.com

PROFESSIONAL SUMMARY:

Cybersecurity Security Operations Center Analyst proven experience in Managing Network Inventory, Applying Security Configurations, Auditing, Designing and Implementing Network Vulnerability Management and Continuous Monitoring Programs in a Cyber Security based environments. I was responsible for monitoring all intrusion detection, and intrusion prevention systems as well as other monitoring tools to determine the validity and severity of alerts generated daily.

TECHNICAL SKILLS:

- Vulnerability Scanning
- Web Application Scanning
- Security Network Monitoring
- Strong verbal communications
- Management functions
- Security Metrics Monitoring
- Security Assessment Reporting
- Firewall Configurations
- Security Tool Configurations
- Vulnerability Management
- Security Scanning
- Continuous Monitoring
- Security Ticketing
- Security Impact Analysis
- Security Requirements
- Security Staffing
- Security Reporting
- TCP/IP Core Protocols
- McAfee SIEM

TECHNICAL TOOLS:

- Malware Bytes
- AVON

- ▪ Blue Coat
- ▪ Cylance
- ▪ ForeScout
- ▪ Tanium EndPoint
- ▪ HP WebInspect Application
- Scanning
- ▪ Akamai
- ▪ Virtru
- ▪ FireEye
- ▪ DISA STIGS
- ▪ McAfee ePO
- ▪ Imperva WAF
- ▪ Iron Key
- ▪ Proof Point
- ▪ Checkpoint
- ▪ Encase
- ▪ SharePoint
- ▪ FIPS-200
- ▪ ISSO Training
- ▪ Security Program Management
- ▪ Splunk Pre-deployment
- Trained
- ▪ O365
- ▪ ServiceNow Ticketing System
- ▪ Tenable Nessus Scanning
- ▪ Okta

▪

EDUCATION:

North Carolina A&T State University

B.S., Business Administration concentration in Management, Completed

CERTIFICATIONS:

▪ CompTIA Security +

▪ CEH

PROFESSIONAL EXPERIENCE:

***Independent Insurance Agent* — (USHA/EQUIS/Teleperformance)**

(03/2020 — Present)

M Powered Strategies – (FRTIB) – HQ Washington, DC

Cybersecurity SOC Analyst- (08/2019 – 01/2020)

- Helping to build a SOC for the organization
- Creating SOC Procedures and workflows
- Helping to select tools and training

Securitas – (AWS) – Chantilly, Va

Security Officer- (12/18 – 08/2019)

- Performed Perimeter & Interior Patrols
- Observed & reported on suspicious activities
- Protected sensitive data systems from physical harm

Federal Communication Commission (FCC) - HQ Washington, DC

Cybersecurity SOC Analyst- (03/2017 – 05/2018)

- Provided analysis and trends of security log data from a large number of heterogeneous security devices
- Reviewed the McAfee Enterprise Security Manager (ESM) dashboards for any alerts encountered during shift
- Monitored the Incident Response (IR) ticket queue and provided incident reports when actionable incident
- occurred
- Provided threat and vulnerability analysis as well as security advisory services
- Reviewed National Cybersecurity and Communications Integration Center (NCCIC) alerts, US-CERT alerts
- Performed log-Integration: Security & Network Devices, Operating Systems, Applications, and Databases
- Conducted HP Web Inspect scans of the entire production network
- Investigated, documented, and reported on information security issues and emerging trends
- Integrated and shared information with other analysts and other teams
- Worked closely with all of the Information Systems Security Officer (ISSO)
- Evaluated ability to identify root cause analysis of performance and unavailability problems
- Conducted Nessus vulnerability, compliance and analytical scans upon request
- Familiar with common protocols and ports for example TCP, UDP, ICMP, SMTP/25 DNS/53, FTP/20, 21,
- HTTP/80, HTTPS/443, RDP/3389

- Omniplex Worldwide Security Services (FCC) – Washington, DC
- Special Security Officer (Part-Time) 10/2014 – 05/2018
- Handled all accident first-responder/investigations, police patrol, ticket/reporting writing, search process
- Provided assistance to customers, employees and visitors
- Oversaw the day-to-day operations
- Observed departed personnel to protect against theft of company property
- Warned violators of rule infractions, such as loitering, smoking or carrying forbidden articles
- Investigated or prepared reports on accidents and incidents
- Managed all CCTV Monitoring/ Switchboard Monitoring

Coastal International Security – Washington, DC

Armed Security Officer – (02/2010 - 02/2014)

- Investigated disturbances and complete daily reports pertaining to all incidents
- Inspected and permitted all authorized persons to enter property
- Monitored security cameras throughout the building of client sites
- Inspected and adjusted all security systems, equipment machinery to ensure operational use
- Prepared a report of daily activities, any incidents occurring on the shift, maintains the building/area security log
- and other irregularities, such as equipment or property damage, theft, presence of unauthorized persons, or
- unusual occurrences
- Detected suspicious activities and watch for criminal acts or client rule infractions at or near assigned post which
- may be a threat to the property, client or employees at the site
- Community Concepts Inc. – Woodbridge, VA
- Direct Support Specialist 7/2009 - 2/2010
- Handled all disable clients; taught soft skills training and supports to adults with disabilities to obtain employment
- Completesd required documentation and reports in compliance with company's policy and regulatory
- requirements
- Maintained healthy and professional communication with mission-based service clients
- Ensured safety and cleanliness of the work environment involvement
- Successfully completed all required orientation, training and health testing
- Analyzed large amounts of information using Excel and other tools for data output