Donte Robinson

Atlanta, GA • 504.405.0927 • dontekendallrobinson@gmail.com • https://www.linkedin.com/in/cyber-donte/

PROFESSIONAL SUMMARY

GIAC certified cybersecurity professional experienced in programming languages, networking, and security tools. Demonstrated experience in cloud security, vulnerability assessment, threat monitoring & remediation, and compliance.

SKILLS

Security: TLS, SSL, IPsec, VPN, MFA, IDS & IPS, Firewalls, SIEM, SAST & DAST, Active Directory, EDR & XDR
Cyber Compliance: PCI DSS, ISO 27001, GDPR, NIST, SOC 2, SOX
Tools: tcpdump, wireshark, Netcat, Nmap, Nessus, Metasploit, Splunk, Burp Suite, Snort, Suricata, pfsense, Splunk
Networking: TCP & IP, UDP, DNS, DHCP, VoIP, Routing, Switching, VLAN, WAN, SDN
Languages: Java, Python, C, C++, SQL
Scripting: PowerShell, BASH
Operating Systems: Kali Linux, Ubuntu Linux, Windows, MacOS

EDUCATION & CERTIFICATIONS

SANS Technology Institute, HBCU+ Cybersecurity Training Academy, Expected: Feb 2024

- **GFACT (SEC275) –** GIAC Foundational Cybersecurity Technologies, July 2023
- **GSEC (SEC401) –** GIAC Security Essentials, Nov 2023
- **GCIH (SEC504) –** GIAC Certified Incident Handler, Expected: Feb 2024

Georgia State University, Bachelor of Science in Computer Science (3.53), Dec 2023

- **Coursework**: Network Security, Security in IoT, Mobile Computing & Wireless Network Security

CodePath Cybersecurity Course (CYB 102), Nov 2023

- Learning to explore and analyze threat data, use SIEM systems to collect security data from endpoints, appropriately correlate data, evaluate and triage events, and use gathered data to perform incident management.

CYBER EXPERIENCE

Cloud Security Engineer Intern, Cantaloupe Inc, Atlanta GA, June 2023 – Dec 2023

- Employed a comprehensive toolset including Microsoft Defender, Azure AD & Sentinel, FortiClient, and Wazuh to proactively monitor and remediate security threats within the company's cloud environments and network endpoints.
- Responsible for creating customized dashboards, for our newly acquired teams, within Tenable.io that provides a consolidated view of vulnerability, compliance, and threat intelligence data retrieved from our Nessus scans.
- Implemented DLP policies via Microsoft Purview for Teams and Office 365, blocking 100+ instances of sensitive data transmission, including PII transmissions like credit card and bank details, and initiated real-time alerts.
- Conducted a Phishing Simulation on over 400 employees followed by Phishing & PII Security Awareness training, to test the company’s defense and raise the awareness of phishing threats.

Home Lab

- Defensive
  - Used tcpdump to capture packets from the network in my home and Wireshark to analyze the captured packets to practice blue team network analysis techniques
  - Set up Wazuh open source SIEM tool in my personal home lab to practice incident response in a simulated corporate environment.
- Offensive
  - Conducted password cracking exercises, utilizing the John tool within the Kali Linux environment, to gain insights into adversarial tactics and strategies.
  - Used the Metasploit platform and Metaploitable machine within Kali Linux to practice identifying port vulnerabilities and test exploits on the services from those vulnerable ports.

Cyber Security Club, Aug 2022 – Dec 2023

- Contributed as the head of a team to complete a network traffic analysis project on our school’s network.
- Taught a group of 5+ novice cybersecurity students on how properly configure a virtual machine using VMware and Azure which is a critical cybersecurity skill.

ADDITIONAL EXPERIENCE

Computer Science Tutor, PAPER Education, Remote, Nov 2022 – Present

- Delivered tutoring to students in fundamental Computer Science concepts like Objected Oriented Programming, Hardware, Algorithms, and Operating Systems thus fostering a deep understanding in the subject matter.