Duwaine Winder

duwainewinder@gmail.com 678.677.1686 Atlanta, GA

Information Security Engineer and IT Network Professional, experienced in managing critical operations and data networks, leading teams of professionals in planning, developing, and maintaining a secure multi-vendor infrastructure. Proficient in identifying, analyzing, and mitigating security incidents, troubleshooting issues, evaluating alternatives, and recommending effective solutions to support robust network architectures.

---------- PROFESSIONAL EXPERIENCE ----------

IBM CORPORATION – Atlanta, GA (04/2019 to 10/2024)
Incident Response Coordinator
Worked with cross-functional teams across the organization responding to security events, ensuring that they are handled as per the company documented policies, procedures and processes in a timely and professional manner.

Handled security events from intake through triage, protection and remediation. Assisted in the technical analysis of security events, producing comprehensive reports that outlined findings, remediation steps, and recommendations for improving overall security posture.

Engaged with and maintained communications with stakeholders at all levels of the organization including IT, legal, management and any affected users, to ensure a cohesive and coordinated response to security events.

- Provided Technical expertise and insight during security event triage.
- Assisted in the on-boarding and training of new hires to the Incident Response Team.
- Assisted in the creation and maintenance of Playbooks/Runbooks and KB's.
- Review log-based data, both in raw form and utilizing SIEM or aggregation tools.
- Employ forensically sound principals for evidence handling and chain of custody.
- Perform live network assessments using packet capture and analysis software tools.

TOOLS: *Crowdstrike, Microsoft Defender, Microsoft Intune, JAMF, MaaS360, Proofpoint Protection Server, Proofpoint TAP (Targeted Attack Protection), QSOAR, Beekeeper, Magna: Built on top of Kibana (data visualization tool), Wireshark.*

IBM CORPORATION – Atlanta, GA (12/2013 to 03/2019)
Network Security Analyst
- Functioned as the on-duty focal/lead for the assigned shift.
- Responsible for providing complex IT Security services to clients within the IBM Managed Security Services organization.
- Ensure Confidentiality, Integrity and Availability of data and critical Information Technology services.
- Perform multiple assigned technical tasks including research, analysis, troubleshooting, system integration, and complex root cause analysis of managed security solutions.

- Configure and administer firewall and Unified Threat Management (UTM) Systems/platforms include; Checkpoint, Cisco PIX, Cisco ASA, Cisco ISR, Juniper Netscreen, Juniper SRX, Fortigate, Palo Alto.

---------- EDUCATIONAL BACKGROUND ----------

MISM– **Information Systems Management** – Keller Graduate School/DeVry University
MNCM**- Network & Communications Management -** Keller Graduate Sch./DeVry Univ
MBA**- International Business -** University of Miami
BS**- Electronics Engineering Technology -** DeVry Institute of Technology

---------- CERTIFICATIONS ----------

Current:
AWS Certified Solutions Architect Associate
GIAC GCLD Cloud Security Essentials
AWS Certified Cloud Practitioner
ISC2 Certified in CyberSecurity
IBM Developer Skills Network - Cloud Core
IBM Security & Privacy by Design
IBM Think Like a Hacker

Expired:
Cisco Certified Network Professional (Voice) / Cisco Certified Network Associate (Route/Switch, Voice, Security)) / Cisco Certified Design Associate (CCDA) / Juniper Networks Certified (JNCIA-Junos) / Palo Alto Networks Certified (ACE)