RAKEEM DAWSON

New Jersey | NYC Metro | Remote U.S. | Open to relocation to the Washington, DC metro area

PROFESSIONAL SUMMARY

Cybersecurity professional transitioning from 9+ years in enterprise IT operations, including identity lifecycle administration for 500+ Microsoft Entra ID accounts. Experience supporting MFA, Conditional Access, privileged-access procedures, Linux systems, endpoint hardening, incident escalation, and IT/OT access controls. Hands-on labs in Microsoft Sentinel and KQL detection, Wazuh, and Nessus-based vulnerability management. CompTIA CySA+, Project+, and ISC2 SSCP; B.S. in Cybersecurity and Information Assurance in progress.

TECHNICAL SKILLS

Security Operations & Detection: Microsoft Sentinel, Wazuh, KQL, Windows Security Event logs, alert triage, IOC analysis and enrichment, incident escalation, response runbooks

Identity & Access Management: Microsoft Entra ID/Azure AD, Conditional Access, MFA, RBAC, PAM360, B2B access reviews, account lifecycle administration, least privilege

Vulnerability & Endpoint Security: Tenable Nessus, basic network scanning, CVSS review, remediation planning, endpoint hardening, security baselines, asset inventory

Systems, Cloud & IT Operations: Ubuntu Linux, Windows, SSH, Dell Wyse thin clients, Proxmox, TrueNAS, Microsoft 365, Azure, Oracle Cloud Infrastructure, ServiceNow, Citrix Workspace

Frameworks: MITRE ATT&CK, NIST CSF, NIST SP 800-53, CIS Controls v8, ISO/IEC 27001

Security Labs & Analysis: Splunk, Snort, Wireshark, Nmap, TryHackMe, Hack The Box

PROFESSIONAL EXPERIENCE

IT Support Specialist
Sep 2021 - Nov 2025

Orsted (Offshore Wind Energy) | Newark, NJ / Remote

- Administered identity lifecycle management for 500+ Microsoft Entra ID accounts, including MFA, Conditional Access, B2B access reviews, and least-privilege controls.
- Applied PAM360 and Entra ID procedures for privileged access, verifying identity before credential resets and MFA re-enrollment.
- Investigated and escalated account-compromise indicators, unauthorized authentication attempts, and anomalous endpoint behavior using documented incident-response procedures.
- Authored runbooks for authentication failures, MFA bypass attempts, and privilege-escalation scenarios, serving as a primary security documentation owner for the team.
- Coordinated with SCADA and ICS security teams on organizational standards and access-control boundaries between IT and OT environments.

IT Support Associate II
Mar 2020 - Sep 2021

Amazon, Inc. | Carteret, NJ

- Hardened and deployed 150+ enterprise workstations annually using security baselines, configuration standards, and endpoint-compliance requirements.
- Supported 500+ Ubuntu-based Dell Wyse 5070 thin clients and Kiva workstations across fulfillment-center departments, using Linux command-line utilities and SSH to diagnose operating-system, process, routing, and connectivity issues.
- Compiled thin-client IP inventories and used an approved change-management script template to generate and execute mass reboot operations across 500+ devices; manually recovered offline devices and validated service restoration.
- Resolved wireless disruptions in robotic and Kiva areas by following team runbooks, identifying disassociated access points, connecting to the wireless controller through SSH, performing runbook-directed interface resets, and confirming workstation recovery.
- Diagnosed Ubuntu media servers supporting AMCare, Loss Prevention, and senior operations by reviewing RAID status, kernel logs, memory usage, and SMART data; replaced failed drives under approved changes.
- Rotated pre-shared key (PSK) credentials on PIT trucks under approved changes, transferring credentials by USB, applying them to each vehicle, and confirming reachability on the isolated vendor network.
- Escorted authorized vendors to the MDF for UPS and fire-system inspections while maintaining controlled access to critical infrastructure areas.

IT Equipment Coordinator
Oct 2016 - Mar 2020

Amazon, Inc. | Carteret, NJ

- Managed the IT asset lifecycle from acquisition and secure configuration through maintenance and compliant retirement, maintaining chain-of-custody records.
- Implemented RMA tracking protocols for faulty and end-of-life devices, reducing turnaround time by 20% while maintaining audit documentation.
- Performed systematic pre-shift security and functionality checks to maintain equipment readiness and identify misconfigured or failing hardware before warehouse operations began.

CYBERSECURITY PROJECTS

Vulnerability Management Program Home Lab

Tenable Nessus | VirtualBox | Windows 10 | Ubuntu Server | pfSense

- Built an isolated VirtualBox lab and documented authorized scope and asset inventory for Windows 10, Ubuntu Server 22.04, and pfSense targets.
- Configured and ran a Nessus Essentials Basic Network Scan from Kali Linux against the defined lab targets; reviewed scanner output and documented a remediation-planning workflow.
- Maintained evidence boundaries by withholding unverified severity totals, plugin mappings, and remediation results until they can be validated against an original .nessus export and comparison rescan.

Microsoft Sentinel SIEM Deployment Home Lab

Microsoft Azure | KQL | MITRE ATT&CK

- Deployed Microsoft Sentinel on an Azure Log Analytics workspace, onboarded a Windows endpoint via Azure Monitor Agent, and validated Security Event log ingestion end to end.
- Wrote and tested KQL queries isolating failed-logon activity (Event ID 4625) by source address, target account, and failure status code, separating password guessing from account enumeration.
- Generated controlled test authentication activity to validate query results before analyzing unsolicited traffic; mapped findings to MITRE ATT&CK T1110 and documented triage steps, false-positive conditions, and containment recommendations.

Secured Virtual Lab Environment Home Lab

Proxmox | Windows | Debian Linux | TrueNAS

- Built a multi-VM environment for system hardening, vulnerability assessment, and security training across Windows and Linux hosts.
- Completed adversary-simulation and incident-response labs through TryHackMe and LetsDefend; currently following the Hack The Box SOC Analyst path with hands-on lab exposure to Splunk, Snort, Wireshark, and Nmap.

CERTIFICATIONS

CompTIA CySA+ (CS0-003), 2025 | ISC2 SSCP, 2025 | CompTIA Project+, 2026 | Microsoft Azure Fundamentals (AZ-900), 2025 | Oracle Cloud Infrastructure Foundations Associate, 2025 | LPI Linux Essentials, 2024

EDUCATION

B.S. in Cybersecurity and Information Assurance, In Progress Expected Nov 2026

Western Governors University | Salt Lake City, UT

Internetwork Engineering Certificate | PC AGE Career Institute, Iselin, NJ

PROFESSIONAL AFFILIATIONS & ACTIVITIES

ISC2 New Jersey Chapter | Active member | **WGU Cybersecurity Club (NIGHTOWLS)** | CTF and security-lab participant