RAKEEM DAWSON

| RakeemSec@pm.me | linkedin.com/in/rakeemdawson | North/Central NJ

SUMMARY

Cybersecurity professional with 9+ years of enterprise IT operations experience across Fortune 500 and energy sector environments, now fully focused on security operations, identity governance, and cloud security. Built and administered identity and access management infrastructure for a hybrid enterprise at Ørsted, enforcing least-privilege access, MFA policy, and PAM controls across 500+ user accounts in Microsoft Entra ID — the exact IAM work that underpins zero-trust architecture, executed in production. Deployed Microsoft Sentinel and Wazuh as end-to-end SIEM platforms, authoring custom KQL and detection rules mapped to MITRE ATT&CK and integrating SOAR automation for incident response workflows. Holds CompTIA CySA+, ISC2 SSCP, and Security+ certifications, with a B.S. in Cybersecurity and Information Assurance from Western Governors University in progress. Actively targeting Security Analyst, and Cloud Security Analyst roles where IAM expertise, SIEM operations, and hands-on incident response translate directly into reduced threat exposure.

TECHNICAL SKILLS

SIEM, Detection & Threat Hunting: Microsoft Sentinel, Wazuh, Splunk, KQL (Kusto Query Language), custom detection rules, log management, alert triage, security event correlation, threat hunting, IOC analysis,

Identity & Access Management (IAM): Microsoft Entra ID, Azure Active Directory, RBAC, Conditional Access, MFA enforcement, PAM360, privileged access management, user provisioning, identity lifecycle management, identity governance, least-privilege access, B2B account management, zero-trust principles

Security Operations & Incident Response: Incident response, alert triage, SOAR automation (Shuffle), case management (TheHive), SOC Tier 1 operations, mean time to respond (MTTR), root cause analysis, escalation procedures

Vulnerability Management & Network Security: Nessus, Snort IDS, Wireshark, Zeek, Nmap, CVSS scoring, vulnerability assessment, intrusion detection, traffic analysis, endpoint hardening, attack surface reduction, network asset inventory

Frameworks & Compliance: MITRE ATT&CK, NIST CSF, ISO 27001, access control auditing, regulatory compliance, least-privilege enforcement, security documentation, entitlement reviews

Cloud & Infrastructure Platforms: Microsoft Azure, , Oracle Cloud Infrastructure, Proxmox, TrueNAS, Debian Linux, Microsoft 365, ServiceNow, Citrix Workspace

PROJECTS

Secured Virtual Lab Environment

Proxmox

- Built and optimized a multi-VM virtual environment on Proxmox for system hardening, vulnerability assessment, and security training across Windows and Linux hosts.
- Conducted structured vulnerability assessments on virtual clients using Nessus, documenting findings with CVSS scores, mitigation strategies, and remediation validation, mirroring deliverables expected in vulnerability analyst and SOC roles.
- Completed adversary simulation, detection methodology, and incident response labs via TryHackMe and HackTheBox, reinforcing practical SOC workflows and blue team analytical skills.

Vulnerability Management Program

Nessus, NIST SP 800-53, ISO/IEC 27001, CIS Controls v8

- Designed and executed a structured vulnerability management program for a multi-asset homelab environment, producing a six-phase documentation framework — spanning asset inventory, scope authorization, scan execution, triage prioritization, remediation ticketing, and MTTR metrics — aligned to NIST SP 800-53 and ISO/IEC 27001:2022.
- Configured and deployed Tenable Nessus to conduct unauthenticated discovery and credentialed advanced network scans across segregated Windows, Debian Linux, and TrueNAS environments, leveraging dedicated service accounts to identify deep, host-level OS and hypervisor vulnerabilities
- Built a remediation and verification process by creating ticket-style records for each CVE, assigning SLA targets, tracking MTTR, and running targeted Nessus verification scans to confirm closure and update the homelab asset inventory.

Microsoft Sentinel SIEM Deployment

Microsoft Azure, KQL, MITRE ATT&CK

- Deployed and configured Microsoft Sentinel in Azure, onboarding Windows hosts and connecting data sources to normalize security event log data and enable centralized security monitoring at enterprise scale.
- Authored custom KQL analytic rules targeting brute force (T1110), privilege escalation (T1068), impossible travel (T1078), and suspicious process execution (T1059), each mapped to MITRE ATT&CK technique IDs to enable structured alert triage and threat prioritization.
- Tuned detection thresholds through iterative testing against Windows Security Event logs and built an end-to-end incident response workflow modeled on SOC Tier 1 operational cadence, documenting each phase from alert trigger through closure.

SOC Automation Lab

Wazuh, Shuffle SOAR, TheHive

- Integrated Wazuh SIEM with Shuffle SOAR and TheHive case management to build an end-to-end automated security operations pipeline spanning threat detection, automated alert routing, case creation, and response playbook execution.
- Configured SOAR playbooks to automate Tier 1 response actions including IOC lookup, alert enrichment, and case escalation, demonstrating full SOC pipeline capability across SIEM, SOAR, and case management platforms and reducing mean time to resolution for simulated incidents.

WORK EXPERIENCE

IT Support Specialist Sep 2021 – Nov 2025

Ørsted (Offshore Wind Energy) · Newark, NJ / Remote

- Administered identity lifecycle management for 500+ user accounts in Microsoft Entra ID, enforcing MFA policies, , and auditing B2B user accounts to maintain least-privilege access and reduce unauthorized access risk.
- Enforced privileged access management (PAM) procedures using PAM360 and Microsoft Entra ID, performing identity verification prior to all credential resets and MFA re-enrollment to prevent social engineering-based account compromise.
- Partnered with SCADA and industrial control systems (ICS) security teams to ensure operational technology (OT) assets adhered to organizational security standards and compliance requirements, including access control boundaries between IT and OT environments.
- Investigated and escalated security incidents including account compromise indicators, unauthorized authentication attempts, and anomalous endpoint behavior, maintaining a 95% SLA resolution rate and applying structured incident response procedures.
- Authored and maintained incident response runbooks covering authentication failures, MFA bypass attempts, and privilege escalation procedures, reducing mean time to respond (MTTR) by 20% and serving as primary security documentation owner for the team.

IT Support Associate II Mar 2020 – Sep 2021

Amazon, Inc. · Carteret, NJ

- Hardened and deployed 150+ enterprise workstations annually, enforcing security baselines, configuration management standards, and endpoint compliance policies to reduce attack surface and minimize provisioning time.
- Investigated and resolved escalated endpoint and network incidents, performing root cause analysis and implementing remediation steps to prevent recurrence and minimize operational risk.
- Maintained network asset inventory and enforced enterprise security and compliance requirements across all managed devices, supporting accurate environmental visibility and audit readiness.
- Delivered on-site IT support across multiple fulfillment facilities, ensuring critical systems remained operational and protected against unauthorized access and configuration drift.

IT Equipment Coordinator Oct 2016 – Mar 2020

Amazon, Inc. · Carteret, NJ

- Managed full IT asset lifecycle including acquisition, secure configuration, maintenance, and compliant retirement, enforcing internal security standards and chain-of-custody controls at every stage.
- Implemented RMA tracking protocols for faulty and end-of-life devices, reducing turnaround time by 20% while maintaining chain-of-custody compliance and audit documentation.
- Maintained 100% equipment operational readiness at shift start through systematic pre-shift security and functionality checks, minimizing risk from misconfigured or failing hardware across a high-volume warehouse environment.

CERTIFICATIONS

- CompTIA CySA+ (CS0-003) — 2025
- CompTIA Security+ — 2022
- Oracle Cloud Infrastructure Foundations Associate — 2025
- ISC2 SSCP — 2025
- Microsoft Azure Fundamentals (AZ-900) — 2025
- LPI Linux Essentials — 2024

EDUCATION

B.S. in Cybersecurity and Information Assurance — *Western Governors University, Salt Lake City, UT*
Internetwork Engineering Certificate — *PC AGE Career Institute, Iselin, NJ*

ADDITIONAL EXPERIENCE

- **ISC2 New Jersey Chapter** — Active member engaging in threat intelligence discussions, emerging vulnerability briefings, and peer networking with security professionals
- **WGU Cybersecurity Club (NIGHTOWLS)** — Active participant in CTF challenges and security labs, reinforcing hands-on offensive and defensive technique awareness