Kevin Dawson

Greensboro, NC | (336) 451-7839 | reachkevindawson@gmail.com |
linkedin.com/in/kevin-dawson-gso

Summary

Cybersecurity professional with hands-on experience implementing security frameworks, managing vulnerabilities, and conducting incident response. Demonstrated success reducing security incidents by 40% through NIST CSF implementation and decreasing phishing risk by 25% via targeted awareness training. Skilled in security monitoring, cloud security architecture, and compliance frameworks. Currently expanding security analytics capabilities through CySA+ certification studies while leveraging Security+, ISC2 CC, Azure Fundamentals, and Qualys VMDR certifications.

Skills

- **Technical Security Skills:** Security Monitoring & Event Analysis, Vulnerability Management & Remediation, Security Framework Implementation (NIST CSF), Cloud Security Architecture (AWS), Identity & Access Management, Endpoint Security & Protection
- **Security Tools:** SIEM: Splunk, Vulnerability Management: Tenable Nessus, Network Security: Suricata, pfSense, Cloud Security: AWS GuardDuty, AWS Detective, AWS Cloudwatch,
- **Microsoft:** Intune, Entra ID, Azure, Active Directory
- **Soft Skills:** Security Awareness Training, Cross-functional Collaboration, Technical Documentation, Professional Communication

Work Experience

IT & Security Consultant | NCCJ of The Triad, Greensboro, NC | Dec 2023 – Present

- Developed and implemented NIST CSF 2.0-aligned security framework that reduced security incidents by 40% within 12 months through systematic control implementation and continuous monitoring.
- Designed and executed security assessments to identify vulnerabilities and compliance gaps, prioritizing remediation based on risk impact and business requirements.
- Enhanced endpoint visibility and reduced vulnerabilities by optimizing Microsoft Entra ID and Intune configurations, securing groups and removing 50 inactive users within 3 months.
- Developed and optimized security policies and procedures, leading a cybersecurity awareness program that reduced phishing risk by 25% over 6 months using targeted GoPhish campaigns.
- Achieved a 95% resolution rate for known security vulnerabilities through proactive security management and monitoring.
- Streamlined technical issue resolution processes, achieving a 30% reduction in average resolution time by enhancing documentation and user support.

- Implemented foundational security controls (VPN, BitLocker) to improve secure remote access and endpoint security.

Desktop Integration Specialist II | Allstate, Winston Salem, NC | Sep 2022 – Present

- Managed security incident response for 1,400+ escalated tickets annually, achieving 84.1% SLA compliance through effective root cause analysis and remediation.
- Collaborated with Cybersecurity team through mentorship program to improve security control implementation and incident detection capabilities.
- Implemented 2FA and IAM controls (Cisco Duo, Active Directory) within an enterprise environment of over 10,000+ users, strengthening endpoint security and access management across the enterprise.
- Transformed incident management workflows, reducing repeat incidents by 10% through self-service solutions and improving team response by 20% via enhanced documentation and SOPs.
- Executed major security-related remediations, including Global Protect VPN and CrowdStrike deployments, enhancing compliance and security posture for over 10,000 users.
- Achieved a 40% reduction in system vulnerabilities through strategic cybersecurity initiatives and deployment of security tools.
- Created and led a yearlong biweekly cybersecurity mentorship program, boosting staff proficiency through hands-on training with security tools and incident response workflows.
- Supported IAM initiatives by auditing Active Directory group memberships and adjusting access rights during lifecycle events and remediations.
- Facilitated cross-department process improvements, optimizing Epic platform usage and enhancing PII security.

E-Commerce Account Coordinator | Home Meridian International, High Point, NC | Dec 2019 – Oct 2021

- Increased revenue by more than $1M during a challenging pandemic while overseeing the development and implementation of innovative e-commerce strategies for Wayfair.com and utilizing detailed data analysis to optimize product margins.
- Enhanced compliance by 75% YoY by normalizing product data to meet international upholstery safety standards, ensuring accurate listings across e-commerce platforms and a reduction in support tickets by 50%.
- Reduced unresolved support tickets by over 50% annually through refined listings, standardized resolution templates, and improved user support.
- Managed product setup and promotional campaigns by collaborating with key e-commerce partners, optimizing product visibility and increasing revenue.

National Retail Account Manager | T-Mobile, Raleigh, NC | Apr 2014 – Dec 2019

- Directed sales operations across 30+ distribution points, increasing T-Mobile's market share through strategic relationship building with local and regional management.
- Implemented enhanced fraud detection measures, protecting sensitive information and reducing customer churn by 8% within 18 months, by adopting stricter payment processing standards.
- Directed asset audits, merchandise audits, presented findings to leadership, and developed action plans for non-compliant partners, ensuring 100% adherence to brand guidelines within 2 months.
- Administered Intune MDM for Apple Store devices, enhancing security compliance and operational reliability through strategic configuration of demonstration endpoints.

Territory Manager | Clearwire, Washington, DC | Mar 2013 – Jan 2014

- Achieved national 'Clearly the Best' award for highest sales volume and margin by driving exceptional leadership and operational excellence.
- Enhanced year-over-year sales by 60% by implementing strategic account management and targeted sales initiatives.
- Managed sales operations across multiple territories by overseeing daily performance, training employees, and executing effective sales strategies.

Projects

- **Vulnerability Management & Compliance Framework Lab:** Simulated real-world vulnerability testing to evaluate system compliance against industry-standard security frameworks like NIST, ISO 27001, and OWASP Top 10. Used Tenable Nessus to run scans, including the CISA scan, to detect and remediate known vulnerabilities, mapping results to control baselines. Created detailed documentation, including an After Action Report, to track risk reduction.
- **AWS Cloud Security & Threat Detection Lab:** Designed and deployed a cloud honeypot on AWS to collect real-world attack data and refine detection strategies using native AWS tools. A T-Pot honeypot was deployed on an EC2 instance to simulate vulnerable services, with traffic segmented using VPCs and security groups. Configured VPC Flow Logs, AWS GuardDuty, and AWS Detective for continuous monitoring and threat detection. Collected RDP/SSH brute-force data and optimized AWS WAF rules to proactively block malicious IPs. Implemented AWS CloudTrail and Config for compliance monitoring and configuration drift detection. Created automated response playbooks using AWS Lambda functions to remediate common security findings.
- **SIEM & IDS/IPS Cybersecurity Simulation Lab:** Built a security operations environment using Splunk, Suricata, pfSense, and Kali Linux to simulate and triage real-time attacks. Configured log collection via Sysmon and Splunk Universal Forwarders, centralizing Windows event logs and network security monitoring logs from Suricata (acting as a network security monitor and IDS/IPS) into Splunk for correlation and visualization. Conducted live

reconnaissance and vulnerability testing with Kali Linux tools (Nmap, Legion) to validate alert fidelity, improving detection coverage and remediation response. Strengthened system defenses by closing exposed ports and disabling unnecessary services as part of incident response simulation. Developed custom detection rules in Suricata to identify targeted attack patterns. Created Splunk dashboards to visualize security metrics and detection performance.

Education & Certifications

- University of North Carolina at Greensboro – Bachelor of Arts in Communication Studies
- CompTIA CySA+ - In Progress (Expected completion: [Month Year])
- CompTIA Security+ - December 2022
- Microsoft Certified: Azure Fundamentals - May 2023
- Qualys VMDR Certified Specialist - September 2023
- ISC2 Certified in Cybersecurity (CC) - February 2023
- CompTIA A+ - March 2023