Philip McDowell
linkedin.com/in/philipmcdowell5

mcdowellphilip5@gmail.com
φ plmcdowe.github.io

Please note: the character phi φ is used to denote items with associated code or documentation, available at my GitHub listed above.

Professional Experience

Network Security & Compliance Engineer (GS-2210-12)   **12/01/2023 – present**
J6 Special Staff – IN Army NG, Joint Forces HQ: 2002 S Holt Rd, Indianapolis

Focused on Future Operations to ensure a secure & compliant enterprise. Develops, tests & documents solutions to enterprise wide changes in the physical & logical domains. Implementation of changes are automated where possible or delivered to the Network Operations Center as a documented solution for step-by-step deployment in Current Operations. Responsible for: IAM & NAC (Forescout Comply to Connect & ISE TACACS+); STIG compliance of network devices; mitigation of CVEs; research & selection of purchases for network device lifecycle plan; participation in technical review of Change Management Requests; documentation of artifacts for Enterprise Mission Assurance Support Service (eMASS).

- Briefed the State Adjutant General with J6 Director on security posture of the enterprise in response to national concern.
- Migrated the entire state's 802.1x & MAB functionality from Cisco Identity Services Engine to Forescout Counteract.
- Developed Bash scripts in IOS.sh to interactively configure switches "on the box" for production deployment. φ
- Developed Bash scripts in IOS.sh to automatically reconfigure switches & routers in production to STIG compliance. φ
- Developing scenario-based training & troubleshooting IOS.sh environments for the Network Administration (NA) team. φ
- Developing scored & ranked "STIG challenge's" in IOS.sh on IOS-XE 17 switches for the Network Administration team. φ
- Configured & deployed C8300 SIP Cisco Unified Border Element routers between ITSP & enterprise CUCM.
- With Network Engineering peers & NA team - planned for, then deployed:
  — C8500 router, C9400 switch, N9K switches & MDS Fibre Channel switches at the Alternate Site in one weekend.
  — C8500 router & C9600 switch at the Primary Site in one weekend.
- Developed pre-admission policies within Forescout for Radius 802.1x & MAB authentication of:
  — Windows clients, printers, Cisco VoIP devices, IOT security & HVAC devices, Wireless Access Points & Wireless Clients.
- Developed PowerShell scripts & policy actions in Forescout to:
  — Identify & remove unauthorized software from Windows clients. φ
  — Identify & remove unauthorized USB device drivers from Windows clients. φ
- Created reporting & alerting policies in Forescout to track:
  — Windows: OS releases; update states; open ports; user sign-on; 802.1X & MAB events; Wired L2 policies; X.509 certs. φ
  — Cisco network device's OS versions & hardware models.
- Leveraged Cisco DNA-C to monitor & alert for Cisco Security Advisories, tuning results based on advisory criteria.
- Recovered DNA-C with Cisco TAC after a failed update killed services.
- Redeployed fresh Identity Services Engine nodes in Primary / Alternate site vSphere platforms.
  — Clustered under primary/backup MNT nodes with five distributed PSN nodes in peer ….
  — Reconfigured TACAS+ Policy Set with greater Authentication & Authorization
- Deployed, for testing purposes, Grafana with Loki to perform Syslog collection, retention; analysis. φ
- Replaced Primary Site's AireOS 5000 series Wireless LAN Controller with Catalyst 9800 WLC.
- Replaced the Primary Site's N5K & 2K datacenter switches with N9K switches. φ
- Started & contributed to the Network Engineering OneNote, documenting all aspects of the enterprise. φ
- Developed Python program to ingest running configs offline & return the required config changes for STIG compliance. φ
- Developed Python program to generate site-specific router configurations at baselined compliance. φ
- Resolved STIGs in the checklists below on over 800 network devices for Command Cyber Readiness Inspection, 2024.
  — (60) IOS & (59) IOS XE Switch – "L2S" & "NDM" rules
  — (53) IOS-XE Router – "RTR" & "NDM" rules
  — (56) NX OS Switch – "L2S" & "NDM" rules
  — (22) WLAN – "Controller Platform"; "Controller Management"; "AP" rules

Senior Network Administrator (GS-2210-12)   **10/01/2021 – 12/01/2023**
Network Operations Center – IN Army NG, Joint Forces HQ: 2002 S Holt Rd, Indianapolis

The GS-12 Team Leader of six GS-11 Network Administrators, responsible for: maintaining classified (SIPR) & unclassified (NIPR) DoD-Information Networks spanning over 60 remote sites, connecting 2,500 daily users, on more than 1,000 Cisco network devices.

- Configured, tested, & lifecycled HAIPE encryption devices for the classified (SIPR) network across the state.

- Oversaw the lifecycle of SIPR networking devices.

- Configured & deployed an IOS-XE C9800 WLC at the organization's alternate site.

- Configured Identity Services Engine; AireOS & Catalyst WLCs for 802.1x authentication to the WLAN by X.509 certs.

- Configured, tested & deployed the lifecycle upgrade of N5K & 2K datacenter switches at the primary site SAN.

- Oversaw the successful lifecycle of the primary site's N7K CORE switch.

- Oversaw the lifecycle of more than 700 access switches across the state.

- Tested, then oversaw the deployment of upgraded wireless access points throughout the state.

- Tested, then oversaw the conversion of edge router MGCP gateways to SIP through DNA-C Jinja2 config templates.

- Utilized DNA-C to modify ssh trustpoints & pki chains to enable token-based TACACS+ authentication to network devices.

- Utilized DNA-C to deploy Survivable Remote Site Telephony (SRST) configurations to all edge-routers.

- Modified network objects & fastpath prefilter rules in Firepower Management Center on ASA devices.

- Reviewed & directed the response to NETCOM Cyber Tasking Orders (CTOs).

Network Administrator (GS-2210-11)   **09/01/2020 – 10/01/2021**
Network Operations Center – IN Army NG, Joint Forces HQ: 2002 S Holt Rd, Indianapolis

One of six GS-11 Network Administrators. This team earned a passing score in the Network Domain of Command Cyber Readiness Inspection, 2021. Responsible for maintaining classified (SIPR) & unclassified (NIPR) DoD-Information Networks, spanning over 60 remote sites, connecting 2,500 daily users, on more than 1,000 Cisco network devices.

- Successfully configured, tested & lifecycled the primary site's Aggregation Services Router.

- Remediated log4j vulnerabilities across Cisco Unified Communications Manager & Identity Services Engine nodes.

- Resolved CAT I STIG ID: *CISC-RT-000130* on over 60 edge routers by creating a Python program which automated the creation of extended ACLs for layer 3 subinterfaces, preventing traffic destined to itself. φ

- Developed a Python program utilizing `debug vpm all` & `power_denial_detected` error to remotely determine if router FXO interfaces have in-service phone lines connected, then automatically rebuilt the edge-router's dial-peers. φ

- Configured, tested & deployed Cisco MDS Fibre Channel switches for data replication at the primary site SAN.

- Resolved CAT II STIG ID: *CISC-L2-000090* on over 700 access switches by creating a Python program to automate the configuration of spanning-tree guard root. φ

- Resolved CAT II STIG findings on all router & switch ACLs by creating a Python program to automate the configuration of `deny ip any any log-input`. φ

- Worked closely with IA team to troubleshoot & deploy changes to extended VoIP ACLs across the state, allowing successful ACAS scans of the VoIP network before 2021 Command Cyber Readiness Inspection.

- Through a coordinated effort with DISA, migrated T1 DSNs to SIP trunks.

Battalion S-6, *Signal Staff Officer* (CPT/O-3)   **08/01/2020 – Present**
HHD, 127th Cyber Protection Battalion

Responsible for: deployment, maintenance & security of network infrastructure facilitating defensive & offensive cyber activities; accounts & access to virtual training environments; planning & orders production for operations involving the battalion, companies, and teams. Recognized for accomplishments during Cyber Shield 2024: in less than 72 hrs. before exercise start - guided the training facility's Network Administrators in resolving misconfigurations on newly-deployed Cisco equipment responsible for the campus WAN; planned & assisted deploying apx. 30 additional switches to extend connectivity; enabled the timely start & successful completion of the two week exercise involving apx. 2,000 participants.

Signal Company Commander (CPT/O-3)   **08/01/2020 – 04/01/2024**
338th Brigade Signal Company, 38th Sustainment Brigade

Selected by the Signal Advisory Board for company command. As Commander of a Brigade Signal Company, ensured the wellbeing & technical proficiency of 37 Signal Soldiers. Additionally, maintained complete accounting of more than $25 million in communications equipment. Planned & oversaw deployment of tactical, satellite band network equipment to provide 24-hour voice & data networks to the 38th Sustainment Brigade. Recognized for integral role in exercise successes.

Battalion S-6 (1LT/O-2)   **01/01/2020 – 08/01/2022**
HHB 2/150 Field Artillery Battalion

Hand-picked by Brigade, Human Resources Staff Officer, to serve as BN S-6. Directed 5 Non-Commissioned Officers & 5 Soldiers to deliver reliable communications on: SINCGARS radio, satellite band Joint Battle Command-Platform (JBC-P), & the Command Post of the Future (CPOF). Integrated 3 Field Artillery Batteries & 1 Support Company into Battalion voice & data networks, enabling the safe & successful execution of numerous live fire exercise. Liable for the maintenance & accountability of S6 equipment, valued more than $1 million. Ensured compliance with Information Assurance (IA) & Security best practices as defined in Army Regulation 25-2.

Joint Network Node Platoon Leader (1LT/O-2)   **11/01/2017 – 12/01/2019**
738th Brigade Signal Company, 219th Engineer Brigade

Rated "Most Qualified" on 2 of 2 Officer Evaluation Reports (OER) while Platoon Leader. Leveraged fully, opportunities for signal training & Soldier counseling to advance the abilities of 2 Non-Commissioned Officers & 14 Soldiers. Maintained accountability & furthered corrective maintenance of equipment valued more than $4 million. Provided voice & data network services throughout 3 Command Post Exercises for Nevada's 17th Sustainment Brigade.

Logistics Project Officer (1LT/O-2)   **07/01/2018 – 09/01/2019**
38th Infantry Division

Managed the logistical requirements of 3 Division exercises, each with over 1,000 participating Soldiers. Precisely created & facilitated the execution of multiple contracts totaling more than $1 million. Directed recoupment of exercise funds from units across the country, ensuring no fiscal-law violations were created. Guided Division mobilization preparation, coordinating movements of equipment & personnel overseas. Oversaw the "Financial Liability Investigation of Property Loss" program, synchronizing FLIPL investigations Division wide, resulting in a faster FLIPL resolution rate.

Assistant Team Leader (SGT/E-5)   **04/17/2008 – 11/15/2017**
D Co. 151 Long Range Surveillance (ABN)

Excelled in numerous positions culminating as Assistant Team Leader. As the ATL, supervised our team's rigorous 24-72 hour planning phase for reconnaissance & surveillance operations – requiring time, task, & knowledge management. On mission, accountable for all team equipment valued more than $500,000, & responsible for team members' welfare. Ultimately, time served as ATL fostered the ability to thrive in small team environments. Developed interpersonal skills & conflict resolution techniques, management abilities, & exacting attention to detail.

Education

Purdue University
West Lafayette, IN   Credit hours: 18 of 30
Professional Master of Science in Computer Science   Concentration: Information & Cyber Security

Summary of Completed Courses

CS 50010 *Foundational Principles of Information Security*:
Data structures; algorithm design; computational complexity; probability theory; number theory; basics of cryptography.

CS 50011 *Introduction to Systems for Information Security*: φ
Security-critical software vulnerabilities in C/C++; basics in architectures; assembly languages; the compiling process.

CS 52600 *Information Security*: φ
authentication & protection models; security kernels; secure programming;
audit; intrusion detection & response; operational & physical security issues; personnel security;
policy formation & enforcement; access controls; identification & authentication; classification & trust modeling; risk assessment.

CS 52900 *Security Analytics*: φ
machine learning algorithms - classification trees, logistic regression, naive Bayes, KNN, SVM;
Neural Networks - Feed Forward, Convolutional, & Recurrence; the application of these algorithms to security tasks;
various exploitation techniques of several models including practical exercise in the generation of targeted & non-targeted adversarial images; application of defensive techniques to mitigate the effectiveness of those images.

CS 54100 *Database Systems*: φ
Logical design of database systems; entity-relationship model; semantic model; relational model; hierarchical model; network model.
Implementations of the models; design theory for relational databases; design of query languages; use of semantics for query optimization.
Design & verification of integrity assertions & security; intelligent query processing and database machines.

CS 55500 *Cryptography*: φ
Concepts & principles of cryptography & data security; principles of secrecy systems; classical cryptographic systems; Data Encryption Standard (DES); public-key encryption; privacy-enhanced email; digital signatures. Proprietary software protection; information theory and number theory; complexity bounds on encryption; key escrow; traffic analysis; attacks against encryption; basic legal issues; e-commerce; and the role of protocols

---

Indiana University   **05/06/2017**
Bloomington, IN   Credit hours: 171
Bachelor of Science in Informatics, Minor in Business   GPA: 3.19

Relevant Course Work

I-101 Introduction to Informatics	I-202 Social Informatics
I-210 Information Infrastructure I	I-211 Information Infrastructure II
I-300 HCI/Interaction Design	I-308 Information Representation
I-400 Prototyping with Arduino Tools	I-407 Intro to Health Informatics
I-453 Computer & Information Ethics	I-494 Design & Dev of an Info System
I-495 Design & Dev of an Info System	

Ivy Tech Community College   **12/14/2013**
Associate of Science in Business Administration

Certifications
CISSP	(1867476)	05/2025 – 05/2028
CCNA 200-301	(CSCO14325030)	03/2023 – 03/2026
CompTIA Security+ SY0-501 ce	(COMP001021335961)	06/2018 – 06/2027

Training
Comply-to-Connect Enhanced Forescout Certified Processional (FSCP)	02/2024

Professional Development & Leadership Training
Basic Training	08/29/2008
Infantry School	08/28/2009
Basic Airborne Course	09/18/2009
Basic Leaders Course	01/30/2015
Officer Candidate School	09/28/2017
Signal Basic Officer Leaders Course	06/07/2018