Arkansas's Cyber Center of Excellence
DIS State Cybersecurity Office
SCSO@arkansas.gov

Summer 2025 Training Catalog

last updated on 6/6/25

Executive Threat Briefing with CrowdStrike

Date	06/10/25	Time	10:00 a.m. – 11:00 a.m.
Location	Virtual		
Registration	https://forms.office.com/g/iGZ1vtKhsd		
Presenter Name	CrowdStrike		
Session Title	Executive Threat Briefing with CrowdStrike		
Session Description	The Executive Threat Briefing provides senior leaders with critical insights into the latest cyber threats targeting organizations, highlighting emerging attack vectors, trends, and key vulnerabilities. Led by CrowdStrike experts, this session will equip executives with the knowledge and tools to make informed decisions on cybersecurity strategy, risk management, and organizational preparedness. Attendees will gain actionable intelligence to safeguard their enterprises against sophisticated threats, all while fostering a culture of resilience at the leadership level.		
Min. Requirements	No minimum skills required.		
Targeted Audience	IT Staff, Non-technical Staff, Senior Leadership	Num. of Participants	300
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K1139: Knowledge of cybersecurity threats and vulnerabilities • T1456: Determine the impact of threats on cybersecurity		

Cisco Networking Academy Ethical Hacking Cohort

Date	05/30/25 - 10/31/25	Time	11:00 a.m. - 12:00 p.m. on Fridays
Location	Virtual		
Registration	https://forms.office.com/g/RV7vmtCgdu		
Presenter Name	Ray Girdler, John Dulaney, & Matt Pipkins		
Session Title	Cisco Networking Academy Ethical Hacking Cohort		
Session Description	This cohort is designed to guide you through the Cisco Networking Academy Ethical Hacker course, equipping you with the skills necessary for offensive security. You'll work through one self-paced module each week, then gather every Friday for group discussions to ask questions, share real-world context, and deepen your understanding of the material. The goal of this cohort is to earn the Cisco Verified Offensive Security Certificate in Ethical Hacking. The course is free, with a low-cost Capture the Flag (CTF) activity required at the end to complete certification (approximately $100-200). Participants should expect to commit around 4 hours per week to complete the course and engage in cohort activities. For more information, visit the course overview here: https://www.netacad.com/courses/ethical-hacker?courseLang=en-US&instance_id=85a1054d-1b5a-4e4a-bd0e-a3606e5a42ca		
Min. Requirements	There are no prerequisites, but an intermediate understanding of networking and cybersecurity is recommended.		
Targeted Audience	IT Staff	Num. of Participants	25
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0797: Knowledge of ethical hacking tools and techniques • K0882: Knowledge of ethical hacking principles and practices • K0955: Knowledge of penetration testing principles and practices • K0956: Knowledge of penetration testing tools and techniques • K1085: Knowledge of exploitation tools and techniques • K1087: Knowledge of social engineering tools and techniques		

NCPC Cybersecurity First Responder

Date	07/21/25 - 07/24/25 (4 days)	Time	8:00 a.m. - 5:00 p.m.
Location	Riverview School District, 820 Raider Drive, Searcy, AR 72143		
Registration	https://cybersecuritydefenseinitiative.org/registration/		
Presenter Name	National Cybersecurity Preparedness Consortium (NCPC)		
Session Title	Cybersecurity First Responder		
Session Description	Cybersecurity First Responder is an intermediate-level course designed for technical personnel who are first responders to any type of cyber-based attack against our nation's critical cyber infrastructure. Blended learning methods are utilized, to include a balance of classroom lecture, hands-on laboratory exercises, and the use of cyberterrorism response tools against real world simulated cyber-attacks. Students learn the proper steps of an incident response to include incident assessment, detection and analysis, and the containing, eradicating, and recovering process from a system or network-based attack. **Upon successful completion of this course, participants will be able to:** • Define steps for handling cybersecurity attacks, including incident assessment, detection and analysis for security incidents, and containing, eradicating and recovering from a system or network-based attack • Identify, define and practice with tools and resources required in the cybersecurity incident response process in order to accurately and successfully detect, analyze and mitigate a cyberattack • Describe the CFR process to include emergency assessment, containment, eradication, restoration and the post-emergency response • Describe secondary incident response techniques and the proper integration of these activities into the CFR process • Define the proper techniques used to properly review, critique and build upon the CFR process through a series of review meetings and lessons learned methods		
Min. Requirements	Any experience with handling cyber-incidents; plus, a minimum three years' experience as a system or network administrator, or a minimum of four years' experience as a cybersecurity professional.		
Targeted Audience	IT Staff	Num. of Participants	35
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0724: Knowledge of incident response principles and practices • K0725: Knowledge of incident response tools and techniques • K0823: Knowledge of incident response policies and procedures • K0824: Knowledge of incident response roles and responsibilities • S0806: Skill in performing incident responses • T0510: Coordinate incident response functions		

Introduction to Networking

Date	7/30/25 - 8/1/25 (3 days)	Time	8:30 a.m. - 4:00 p.m.
Location	University of Arkansas at Little Rock, 2801 S. University Avenue, Little Rock, AR 72204		
Registration	https://forms.office.com/g/KAgiW5BnDU		
Presenter Name	Mike Kelley		
Session Title	Introduction to Networking		
Session Description	This hands-on, three-day course provides a foundational understanding of networking concepts and practices essential for anyone entering or advancing in the field of IT. Through a combination of classroom instruction and guided lab exercises, participants will explore key networking topics, including: • TCP/IP functions and addressing • Spanning Tree Protocol (STP) • Link aggregation • Layer 2 design principles • Port security and controls • Techniques to limit MAC flooding • ARP security • VLAN concepts and configurations • Networking best practices • Common troubleshooting methods This course is ideal for those looking to strengthen their practical and theoretical knowledge of core networking principles in a structured and engaging learning environment. **Instructor Bio:** Mike brings over 38 years of global IT experience, specializing in network and security engineering. A Cisco Certified Internetwork Expert (CCIE) for more than 25 years, Mike has held senior engineering and architect roles at Cisco Systems for nearly 15 years and has worked with multiple Fortune 500 companies. He currently serves as a Solutions Consultant at Palo Alto Networks, where he continues to lead and support large-scale cybersecurity and infrastructure projects.		
Min. Requirements	There are no prerequisites, but participants should have a general understanding of operating systems and basic troubleshooting skills.		
Targeted Audience	IT Staff	Num. of Participants	24
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0008: Knowledge of communication methods, principles, and concepts that support the network environment. • K0229: Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. • K0173: Knowledge of networking protocols and services (e.g., TCP/IP, UDP, DNS, SMTP, SNMP). • T0048: Configure network equipment and services, including switches and routers. • T0340: Troubleshoot network systems when necessary and make improvements to the network. • T0251: Monitor system performance and capacity to ensure reliable operations.		

NCPC Comprehensive Cybersecurity Defense

Date	8/25/25 - 8/28/25 (4 days)	Time	8:00 a.m. - 5:00 p.m.
Location	Public Works Facility, 2601 Dan Avenue, Jonesboro, AR 72401		
Registration	https://cybersecuritydefenseinitiative.org/registration/?course=2728		
Presenter Name	National Cybersecurity Preparedness Consortium (NCPC)		
Session Title	Comprehensive Cybersecurity Defense		
Session Description	Comprehensive Cybersecurity Defense is a basic-level course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. The course introduces students to cyber-defense tools that will assist them in monitoring their computer networks and implementing cybersecurity measures to prevent or greatly reduce the risk of a cyber-based attack. This course integrates hands-on computer lab applications to maximize the student's learning experience. **Course Objectives** • Effectively protect computer networks by a survey of the following: planning and preparation of defenses, installation and administration of defenses, hardening network defenses, monitoring defenses, and testing and modifying defense • Increase understanding of historical perspectives, network design, and emerging methodologies in computer hacking		
Min. Requirements	This course is an intermediate level hands-on course where knowledge and experience is required. Participants should have a minimum of two years' experience as a system or network administrator, or as an IT security specialist. Any experience with penetration testing, plus a minimum of three years' experience as a system or network administrator or an IT security specialist is preferred.		
Targeted Audience	IT Staff	Num. of Participants	35
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K1175: Knowledge of network monitoring tools and techniques • T1560: Mitigate risks in systems and system components		

For questions about the program or course information, contact:

DIS State Cybersecurity Office (SCSO)
Ray Girdler
State IT Security Specialist
Raymond.Girdler@arkansas.gov

Visit the SCSO webpage for more information:
https://transform.ar.gov/information-systems/cybersecurity/