CYBER ARTS AND MEDIA TECHNICIAN

(Existing USDOL Title: Cyber Security Technician/Information Security Analyst)

O*NET-SOC CODE: 15-1212.00 RAPIDS CODE: 2050CB

Competency-Based Minimum 2000 Hours

JAM™ Apprenticeship Program Approved CDLE/USDOL RAP: 2022-CO-111963 ID
Competency-Based Training Outline Contact: Trey Grimes trey@cleoparkerdance.org

Job Function: Safety Guidelines and Ethical Moral Protocols

1 Identify hazards associated with the workplace and record and report in accordance with organizational procedure

2 Understand all workplace safety requirements at all times

3 Understand and maintain all organizational security arrangements and approved procedures

4 Understand and comply with all emergency procedures in accordance with organizational policy Job Function: Cybersecurity Principles, Cyber Threats & Countermeasures Competency Criteria Initial Training Proficient in Task

5 Analyze potential Intrusions; Denial of Service attacks; Apprentice(s) will demonstrate level of efficiencies utilizing open source cyber security software Forensic Toolkit (FTK) approved by Department of Defense (DoD) ; National Initiative Cybersecurity Education (NICE) ;National Institute Standards and Technology NIST

6 Understand Basics of Phishing Attacks in Media, communicate level of knowledge in written project.

7 Understand Preventing unauthorized access network infrastructure within Arts Venues Organizations. Knowledge communicated in written form.

8 Uses principles of Avoiding suspicious and malicious sites in arts/film/media; written communication

9 Displays awareness and understanding Risk Analysis in Arts Infrastructures; proficiencies assessed by knowledge, skills and ability (KSA) in FTK

10 Observes proper mobile device operation for arts media content creation and access and communicates knowledge in written form

11 Identifies and understands computer network defense (CND) utilizing open source vulnerability assessment tools and their capabilities. Assessed by KSA and operation in FTK

12 Demonstrates skills in identifying measures of indicators of system network performance in arts venue infrastructures utilizing software application(s) in Forensic Tool Kit (FTK)

Job Function: Cybersecurity Principles, Cyber Threats & Countermeasures

5 Analyze potential Intrusions; Denial of Service attacks; Apprentice(s) will demonstrate level of efficiencies utilizing open source cyber security software Forensic Toolkit (FTK) approved by Department of Defense (DoD) ; National Initiative Cybersecurity Education (NICE) ;National Institute Standards and Technology NIST

6 Understand Basics of Phishing Attacks in Media, communicate level of knowledge in written project.

7 Understand Preventing unauthorized access network infrastructure within Arts Venues Organizations. Knowledge communicated in written form.

8 Uses principles of Avoiding suspicious and malicious sites in arts/film/media; written communication

9 Displays awareness and understanding Risk Analysis in Arts Infrastructures; proficiencies assessed by knowledge, skills Page • A-24 and ability (KSA) in FTK

10 Observes proper mobile device operation for arts media content creation and access and communicates knowledge in written form

11 Identifies and understands computer network defense (CND) utilizing open source vulnerability assessment tools and their capabilities. Assessed by KSA and operation in FTK

12 Demonstrates skills in identifying measures of indicators of system network performance in arts venue infrastructures utilizing software application(s) in Forensic Tool Kit (FTK)

Job Function: AP Computer Science Principles/Cybersecurity

13 Demonstrates knowledge of current industry methods for evaluating, analysis, and reporting outcomes for cybersecurity solutions. Written communication.

14 Understands art venue/media outlet enterprise information technology (IT) goals and objectives. Observed in written communication.

15 Shows knowledge of new and emerging information technology and information security principles. Utilizes FTK.

16 Understands how cybersecurity is critical in venues/events environment and media content; displayed by policy observations and written communication.

17 Shows knowledge of structured analysis principles and methods by observing and utilizing the appropriate principles and methods on the job.

Job Function: Information Security and Secure Networking in Media

18 Shows knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Criminal Law Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed in written communication.

19 Shows knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures utilizing KSA in FTK software application.

20 Demonstrates knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability in written communication.

21 Demonstrates knowledge of relevant laws, policies, procedures, or governance as they relate to work that may Criminal Law impact critical infrastructure in written communication

22 Shows knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth) in use of FTK software application. Job Function: Steganography and Applied Cryptography in Arts & Media Competency Criteria Initial Training Proficient in Task

23 Demonstrates knowledge of secure coding techniques in use of open source software cybersecurity applications FTK; Linux; WireShark .

24 Shows KSA in integrating black box security testing tools into quality assurance process of software releases in written communication.

25 Shows KSA in using code analysis tools to eradicate bugs utilizing FTK open source software application.

26 Shows knowledge, skills, abilities of root cause analysis for incidents in open source software application FTK.

27 Shows knowledge of software-related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization) utilizing FTK. Job Function: Data Structures Competency Criteria Initial Training Proficient in Task

28 Shows KSA of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth) in both FTK open source software application and written communication.

29 Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability shown in written communication.

30 Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures in written communication.

31 Knowledge of secure software deployment methodologies, tools, and practices in written communication.

32 Analyze user needs and requirements to plan system architecture in written form.

33 Develop information assurance (IA) designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and TOP SECRET) in written communication.

Job Function: Symmetric & Public Key Encryption Competency Criteria Initial Training Proficient in Task

34 Knowledge, Skills and Abilities (KSA) of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange[IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]), Utilize FTK; SANS Investigative Forensic Toolkit (SIFT); Sleuth Forensic Open Source applications.

35 Displays KSA of cryptology in FTK; SIFT software applications

36 Shows Knowledge of the Security Assessment and Authorization (SA&A) process in FTK; Sleuth

37 Shows Knowledge of industry-standard and organizationally accepted analysis principles and methods utilizing FTK; Sleuth; SIFT software applications.

38 Knowledge of organization's enterprise information security architecture system in written communication.

Job Function: Risk Analysis & Management; Intrusion Detection

39 Shows KSA of risk management processes, including steps and methods for assessing risk in FTK.

40 Demonstrates knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools in use of FTK; Sleuth; SIFT Tools and software applications.

41 Demonstrate Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures in written communication.

42 Demonstrate Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools in written communication.

43 Understand continuous analysis to identify network and system vulnerabilities utilizing scenarios and project based modules for arts organizations and media in open source applications FTK and Sleuth tool kits.

44 Knowledge of relevant laws, policies, procedures, or governance as they relate to work that may impact critical infrastructure in written communication

45 Displays knowledge of operations security in written communication

46 Shows knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data in both written communication and project-based formats utilizing FTK and SANS (SIFT).

47 Utilizes knowledge of Privacy Impact Assessments (PIA) in written communication

48 KSA of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS]) in FTK; SIFT; Sleuth toolkits.

49 Explain knowledge of Global Systems for Mobile Communications (GSM) architecture in written communication

50 Explain knowledge of how system components are installed, integrated, and optimized in written communication

51 Explain knowledge of human-computer interaction principles in written communication

52 Explain knowledge of information security systems engineering principles in written communication

53 Display knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management 54 Explain knowledge of organization's evaluation and validation requirements in written communication

Job Function: Cybersecurity Reporting, Collection of Evidence and Chain of Custody

55 Displays knowledge, skills and ability in using information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, and encryption) shown in use of FTK and SIFT software application performance.

56 Shows knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design in software Canvas by creation of chart design.

57 Shows skill in designing security controls based on information assurance (IA) principles and tenets using FTK software.

58 Knowledge of digital rights management in project based content creation utilizing open source software Audacity

59 Shows knowledge, skills and abilities of the characteristics of physical and virtual data storage media utilizing FTK

60 Shows knowledge, skills and abilities (KSA) of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools in FTK software application

61 Shows KSA of digital media sources, characteristics, and uses of the organization’s data in production using FTK

Job Function: Digital Archival Structures, Naming Conventions, Forensics for Arts Media, and Arts

62 Understand and be able to perform indexing/cataloguing, storage, and access of organizational documents and historical materials in open source software application ArchiveSpace.

63 Shows KSA of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs) in written communication

64 Use principal methods, procedures, and techniques of gathering information and producing, reporting, and storing digital archives for arts venues in ArchiveSpace open source software application

65 Use knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption) in ArchiveSpace; FTK

66 Display knowledge of embedded systems for digital archival purposes in use of ArchiveSpace; FTK, SIFT open source software application(s).

Related Technical Instruction Provided By: Trey Grimes

Location: Online/ Classroom Competency Based

Course/Description:

Apprenticeship Orientation Including Workplace Safety and Anti-Harassment Training
CEH-Lab Work Basics

Linux Basics

UNIX Basics

PEN Basics

Digital Forensics Advanced (Arts/Media/Entertainment)

Network Server Configuration

Risk Analysis

Risk Management/Reporting

E-Discovery/Litigation