

COMPUTER NETWORK DEFENSE ANALYST

RESOURCE CATEGORY	Cybersecurity
RESOURCE KIND	Not Specified
OVERALL FUNCTION	
COMPOSITION AND ORDERING SPECIFICATIONS	1. This position can be ordered as a single resource or in conjunction with a NIMS typed team (Cyber Incident Response Team). 2. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment 3. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days

Each type of resource builds on the qualifications of the type below it. For example, Type 1 qualifications include the qualifications in Type 2, plus an increase in capability. Type 1 is the highest qualification level.

COMPONENT	SINGLE TYPE	NOTES
DESCRIPTION	The Computer Network Defense (CND) Analyst: 1. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or may possibly occur within the network 2. Protects information, information systems, and networks from threats	Not Specified
EDUCATION	Not Specified	Not Specified
TRAINING	Completion of the following: 1. IS-100: Introduction to Incident Command System, ICS-100 2. IS-200: Incident Command System for Single Resources and Initial Action Incidents 3. IS-700: National Incident Management System, An Introduction 4. IS-800: National Response Framework, An Introduction 5. Computer defense in prevention, detection, and response training as the Agency Having Jurisdiction (AHJ) determines	Not Specified

Superseded

COMPONENT	SINGLE TYPE	NOTES
EXPERIENCE	<p>AHJ-validated knowledge, skills, and abilities demonstrated in the following areas:</p> <ol style="list-style-type: none"> 1. CND in-depth principles 2. CND and vulnerability assessment tools, including open source tools, and their capabilities 3. Encryption 4. Data backup, types of backups, and recovery concepts and tools 5. Host and network access controls 6. Intrusion Detection System (IDS) tools and applications 7. Incident response and handling methodologies 8. Information assurance (IA) principles and organizational needs that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation 9. Intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies 10. Network protocols 11. Network traffic analysis methods 12. New and emerging information technology (IT) and information security technologies 13. Traffic flow patterns across the network 14. Penetration testing principles, tools, and techniques 15. Policy-based and risk adaptive access controls 16. Programming language structures and logic for current production platforms 17. System and application security threats and vulnerabilities 18. Security management 19. Content development 20. CND service provider reporting structure and processes 21. Virtual Private Network (VPN) security 22. Network attack and the relationship to both threats and vulnerabilities 23. Common adversary tactics, techniques, and procedures (TTP) in assigned area of responsibility 24. Common network tools 25. Defense-in-depth principles and network security architecture 26. Different types of network communication 27. File extensions 28. Common operating systems command lines 29. Collection management processes, capabilities, and limitations 30. Front-end collection systems, including network traffic collection, filtering, and selection 31. CND policies, procedures, and regulation 32. Common cyber-attack vectors on the network layer 33. Different classes of cyber attacks 34. Different operational threat environments <p>(Continued)</p>	<p>The knowledge, skills, and abilities align with the National Initiative for Cyber Education (NICE), National Cybersecurity Workforce Framework.</p>

Superseded

COMPONENT	SINGLE TYPE	NOTES
EXPERIENCE	<p>(Continued)</p> <p>35. Troubleshooting basic systems and identifying operating systems-related issues</p> <p>36. Basic system administration, network, and operating system hardening techniques</p> <p>37. Applicable laws relevant to work performed</p> <p>38. General cyber-attack stages</p> <p>39. Network security architecture concepts, including topology, protocols, components, and principles</p> <p>40. Encryption methodologies</p> <p>41. Signature implementation impact for viruses, malware, and attacks</p> <p>42. Operating system ports and services</p> <p>43. Various IDS technologies such as host-based network passive IDS, network active IDS, unified threat management, and web application firewalls</p> <p>44. Network firewalls and firewalling techniques</p> <p>45. Reading and interpreting signatures for viruses, malware, and attacks</p> <p>46. Utilizing virtual networks for testing</p> <p>47. Identifying common encoding techniques</p> <p>48. Reading hexadecimal data</p> <p>49. Data reduction</p> <p>50. Configuring and utilizing network protection components</p> <p>51. Using network analysis tools to identify vulnerabilities</p> <p>52. Recognizing and categorizing types of vulnerabilities and associated attack</p> <p>53. Collecting data from a variety of CND resources</p> <p>54. Sub-netting tools</p> <p>55. Protocol analyzers</p> <p>56. Incident handling methodologies</p> <p>57. Performing packet-level analysis using appropriate tools</p> <p>58. Network mapping and recreating network topologies</p> <p>59. Detecting host and network-based intrusions via intrusion detection technologies</p> <p>60. Developing and deploying signatures</p> <p>61. Conducting open source research for troubleshooting novel client-level problems</p> <p>62. Conducting vulnerability scans and recognizing vulnerabilities in security systems</p> <p>63. Interpreting and incorporating data from multiple tool sources</p> <p>64. Integrating and managing network firewall technologies</p> <p>65. Integrating and managing other computer defense tools and techniques to including intrusion detection, prevention, data loss prevention, white and blacklisting, correlation, and alerting</p> <p>66. Integrating the collection of network and other sensor logs for use with log</p> <p>(Continued)</p>	

Superseded

COMPONENT	SINGLE TYPE	NOTES
EXPERIENCE	<p>(Continued) analysis tools</p> <p>AHJ-documented and validated experience demonstrated in the following areas:</p> <ol style="list-style-type: none"> 1. Developing content for CND tools 2. Characterizing and analyzing network traffic to identify anomalous activity and potential threats to network resources 3. Coordinating with enterprise-wide CND staff to validate network alerts 4. Monitoring external data sources to maintain currency of CND threat condition and determine which security issues may have an impact on the enterprise 5. Documenting and escalating incidents that may cause ongoing and immediate impact to the environment 6. Performing CND trend analysis and reporting 7. Performing event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack 8. Providing daily summary reports of network events and activity relevant to CND practices 9. Receiving and analyzing network alerts from various sources within the enterprise and determining possible causes of such alerts 10. Providing timely detection, identification, and alerts of possible attacks and intrusions, anomalous activities, and misuse activities, and distinguishing these incidents and events from benign activities 11. Using CND tools for continual monitoring and analysis of system activity to identify malicious activity 12. Analyzing identified malicious activity to determine weaknesses exploited, exploitation methods, and effects on system and information 13. Employing approved defense-in-depth principles and practices 14. Determining appropriate course of action in response to identified and analyzed anomalous network activity conducting tests of IA safeguards in accordance with established test plans and procedures 15. Determining TTP for intrusion sets 16. Examining network topologies to understand data flows through the network 17. Recommending computing environment vulnerability corrections 18. Identifying and analyzing anomalies in network traffic using metadata 19. Conducting research, analysis, and correlation across a wide variety of all source data sets 20. Validating IDS alerts against network traffic using packet analysis tools 21. Triaging malware 22. Identifying applications and operating systems of a network device based on network traffic <p>(Continued)</p>	

Superseded

COMPONENT	SINGLE TYPE	NOTES
EXPERIENCE	(Continued) 23. Reconstructing a malicious attack or activity based on network traffic 24. Identifying network mapping and operating system fingerprinting activities	
PHYSICAL/MEDICAL FITNESS	Not Specified	Not Specified
CURRENCY	1. Participates in exercise, drill, or simulation at least once every year 2. Background checks as applicable law permits and requires 3. Active security clearance	Provider must carry out and use any background checks as applicable law specifies. This may include a background check completed within past 12 months; sex-offender registry check; and a local, state, and a local, state, and national criminal history.
PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS	1. Technical qualifications equivalent to Department of Defense Directive (DoDD) 8570 Level 2 2. Information Assurance Certification 3. Intrusion Analyst Certification 4. Computer Network Defense	Not Specified

Superseded



Position Qualification for Cybersecurity Cybersecurity

NOTES

Nationally typed resources represent the minimum criteria for the associated category.

REFERENCES

1. FEMA, NIMS 508: Cyber Incident Response Team
2. National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014
3. Department of Defense Directive (DoDD), 8570 and Global Information Assurance Certification (GAIC), January 2014

Superseded