**Title:** Cyber Protection Team Master Host Analyst (Microsoft Windows)

**Location:** Washington, D.C.

**Clearance:** TS/SCI with a CI Polygraph

**Responsibilities:**

* Analyze Windows-based file systems, permissions, and operation system configurations in order to detect vulnerabilities and intrusions
* Capture memory of individual processes on Windows-based systems, perform analysis using built-in tools and capabilities
* Navigate and search Windows file system structure and common processes for vulnerabilities, anomalies, backdoors, rootkits, remote-access tools, malware, etc.
* Perform initial triage procedures on potentially malicious/compromised Windows systems and follow best business practices
* Patch system vulnerabilities to ensure information is safeguarded against outside parties
* Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements
* Conduct network and system level reconnaissance and vulnerability analysis of other systems within a network
* Identify and conduct network mapping and operating system (OS) fingerprinting activities
* Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity
* Conduct open source data collection via various online tools
* Edit or execute scripts (e.g., PowerShell PERL, VBScript) on Windows systems to perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data
* Deploy cyber tools to a target Windows system and utilize them once deployed (e.g., backdoors, sniffers)
* Determine and document software patches or the extent of releases that would leave Windows software vulnerable
* Identify Windows applications and operating systems of a network device based on network traffic
* Validate intrusion detection system (IDS) alerts
* Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces
* Evaluate Windows system security architecture and its design against cyberspace threats as identified in operational and acquisition documents
* Perform security reviews and identify gaps in Windows environment security architecture and develop a security risk management plan
* Provide and maintain CPT documentation for TTPs as inputs to training programs
* Work with stakeholders to resolve Windows computer security incidents and vulnerability compliance
* Identify potential points of strength and vulnerability among Windows segments of a network map
* Assist in the construction of signatures which can be implemented on cyber defense tools in response to new or observed threats within a given Windows network enclave
* Detect exploits against targeted networks and Windows hosts and react accordingly
* Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on Windows systems and information
* Isolate, extract, analyze, remove, and document malware on Windows systems
* Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan
* Plan and recommend modifications or adjustments based on exercise results or system environment

**Requirements:**

* Bachelor's degree desired, but not required
* 7+ years of experience in any combination of cyber technology, cybersecurity, offensive cyber operations, penetration testing, coding/scripting, vulnerability assessments, network/system administration, or related fields
* 4+ years of experience conducting or supporting Cyber Mission Forces exercises
* Must possess advanced knowledge of Enterprise Windows Services and the security configuration of them
* Experience with Virtualized Software Security and PowerShell for developing common automation tasks and custom modules and functions in order to identify anomalies or suspicious machines
* 5+ years of experience as a Certified Senior Level Analyst
* Must be compliant with:
* Windows System Analyst Senior Level Certification
* Advanced Security Onion Course Certification
* Advanced Network Forensic and Analysis Certification
* GIAC Certifications: GCIA, GSNA, GNFA
* Offensive Security Certified Practitioner (OSCP)
* Offensive Security Certified Expert (OSCE)
* SIEM with Tactical Analytics (SEC555) completion
* Active DOD 8570 IAT Level III
* Active TS/SCI security clearance with a CI polygraph, or the ability to obtain and maintain a CI polygraph
* As a contingency to employment at NetCentrics, all candidates who are given offers must successfully pass a background investigation including criminal history and reference checks

This employer participates in E-Verify and will provide the federal government with your Form I-9 information to confirm that you are authorized to work in the U.S. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, veteran status or on the basis of disability.

*Equal Opportunity Employer/Veterans/Disabled*