Position Description

Title: Security Operations Center (SOC) Analyst (Intern)
FLSA Classification:
Reports To:
Supervises: No direct report
Employee Printed Name:
Employee Signature:
Manager Signature:

Position Primary Purpose: The SOC Analyst (Intern) position is responsible for monitoring and analyzing network data to ensure secure computing in the NWCU enterprise. NWCU seeks an individual who can bring security analysis and incident response experience to support daily operations in order to assist in the growth and maturation of the information security program. The incumbent will be responsible for investigating anomalies and discrepancies, creating new detection methodologies, and provided support for NWCU incident response and monitoring functions.

Essential Functions:
• Monitor SIEM, IDS/IPS, antivirus, vulnerability management, and firewall dashboards in order to evaluate the confidentiality, integrity, and availability of enterprise information systems
• Perform audit, analysis, and reporting on system logs and records to ensure organizational awareness of information security status
• Demonstrate working knowledge of information technology, to include: information security, system and/or network administration, forensics, remediation, and incident response
• Conduct research to ensure the detection, investigation, reporting, and mitigation of suspicious activity; compile trend analysis reports and metrics
• Respond to computer security incidents by collecting, analyzing, and preserving digital evidence to ensure that incidents are recorded and tracked in accordance with NWCU requirements

Demonstrated Abilities:
• Experience monitoring SIEM, IDS/IPS, antivirus, vulnerability management, and/or firewall interfaces
• Ability to act appropriately, in a professional manner, in any situation
• Time management and multitasking skills, and excellent attention to detail
• Analytical, critical thinking, and investigative experience, especially analyzing network traffic and IDS events for malicious intent
• Strong collaborative skills and proven ability to work in a diverse team of security professionals

Position Qualifications:
Education: Bachelor's degree in Cyber Security, Computer Science, Management Information System (MIS), or related field

Certifications: CompTIA Security+, Network+, and/or Cloud+ desired; vendor-specific security certifications will be considered
**Working Conditions:**

**Physical:** Continuous standing and/or sitting for long periods of time when providing services or performing other duties related to the position. Occasional lifting up to ten pounds. Occasional bending, squatting, or kneeling to reach supplies on ground level. Occasional reaching above shoulder level to reach supplies overhead. Continuous use of hands in repetitive tasks such as simple grasping, twisting/turning of wrists; finger dexterity to perform various accounting duties such as using a 10 key calculator, typing, and entering data into the computer system. Continuous speaking and hearing for interactions with members and co-workers. Frequent clarity of vision at twenty inches or less for normal use of computer systems. Occasional clarity of vision at twenty feet or more for security purposes.

**Mental:** Continuous alertness, precision, and concentration to ensure accuracy and thoroughness of documents and transactions. Continuous alertness of surroundings for security purposes. Frequent performance of basic numeric calculations, as well as writing, reading, comparing, and analyzing. Frequent use of judgement, reasoning, patience, and negotiation. Continuous memory demands in recalling Credit Union policies, services, and state and federal regulations.

**Environmental:** Length of workday is unpredictable. May have to work long hours because of computer failure, unusual activity, or extended business meetings. Exposed to potentially hazardous conditions. Receives detailed instructions and procedures to be followed to minimize risk. Occasional travel may be required.