NDIT Cybersecurity Apprentice

Information Services I

The North Dakota Information Technology (NDIT) team supports the IT business needs of state government, K-12, and higher education with a purpose of Empowering People, Improving Lives, and Inspiring Success. With technology changing virtually every job and every industry, the NDIT Team's vision is to be a trusted business advisor to state agencies, with goals of providing a world-class government experience, securing all government-held data, and delivering the most efficient services in the country.

North Dakota Information Technology focuses on solving problems and achieving business objectives through a holistic approach to people, process and technology. The North Dakota Information Technology team, part of the Executive Branch of state government, includes more than 500 IT professionals who are committed to providing world-class technology and service to North Dakota's citizens and state agencies.

Purpose

The Information Security Analyst provides monitoring, investigation and verifies that data/systems are accessed according to the appropriate policy. This position will assist in the technical analysis and recommendations for remediation of Operating System, Network and other enterprise events.

Incident Response/Threat Hunting – 55%

- Monitor and serve as an incident handler to identify, investigate, mitigate, and respond to cybersecurity events and incidents impacting the network or endpoints.
- Document evidence collected, actions taken during the incident response process, and write incident reports for management, incident stakeholders, and to facilitate lessons learned.
- Provide de-obfuscation and indicators of compromise during an active incident.
- Evaluate threat information, discover vulnerable systems, propose mitigation and response actions, and present threat information to stakeholders.

- Perform digital forensics of systems to collect, preserve, examine, analyze, and report on evidence in support of incident response, cyber threat intelligence development, and applicable legal or compliance requirements.

- Utilize static and dynamic malware analysis tools to examine potential malware samples to understand their impact, extract indicators of compromise, and to identify the latest malware behaviors and techniques.

Tabletop Exercises – 15%

- Collaborate with other teams to develop a threat hunting strategy based on cyber threat intelligence and conduct threat hunting exercises to proactively detect and isolate threats that evade existing security solutions.
- Participate in tabletop, cyber range, and purple team exercises to improve skillsets, develop a cooperative mindset, and enhance information sharing within the organization.
- Combine threat intel and exploitation analysis to perform planned and authorized testing of computer systems, networks, and web applications.
- Assess countermeasures and controls by attempting to breach security with the same tactics, techniques, and procedures an adversary may use.

Training and Development – 20%

- Actively pursue training to gain the key skills, competencies, and knowledge required to excel in the position.
- Participate in 1-on-1 conversations with your manager and practice self-reflection to identify areas of development in order to prepare you for future success.

Education

Minimum of one of the following:

- Currently be in enrolled in a cybersecurity program through Lake Region State College.

For more information, contact Kelsey Fetterman. kfetterman@nd.gov.