Cyber Security

What is it?

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Why is Cyber Security important?

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber-attacks and digital spying are the top threat to national security, eclipsing terrorism.

A job that I found interesting and the requirements and qualifications needed. (Indeed.com)

Position Description

As a Cyber Intelligence Analyst, you will process vulnerability and threat data from a variety of internal and external sources to provide actionable intelligence to internal consumers. These consumers use the information to implement countermeasures and maintain and enhance the defenses for our information systems and resources. In this important position, you will keep it possible for the organization to defend its assets with clear vision and situational awareness in a persistent, dynamic, and highly complex threat environment. Specific responsibilities will include the following:

- Monitoring and processing various sources to produce actionable intelligence for multiple consumers
- Supporting the development of new sources as necessary
- Continuously evaluating existing sources for value and supporting decision-making related to the future use of those sources
- Mentoring and developing less experienced team members
- Monitoring the team's output for quality and value
- Supporting the creation and implementation of new processes as appropriate
- Staying current on cyber security best practices, news, issues, vulnerabilities and threats (specifically as they apply to the healthcare and financial industries)
- Supporting relationships with multiple vendors
- Supporting relationships with partner teams
- Fulfilling routine and ad-hoc reporting requests
- Conducting advanced analytical research efforts
- Conducting briefings as needed

- Supporting activities related to the implementation and use of tools for intelligence gathering, analysis, and reporting

Requirements

To be considered for this position, applicants need to meet the qualifications listed in this posting.

- Demonstrated critical thinking and problem solving skills
- Proven communication skills, both written and verbal, to both business and technology audiences
- Knowledge of data correlation techniques
- Knowledge of processes, procedures, and methods to research, analyze, and disseminate open source intelligence information
- Intelligence analysis experience using intelligence analysis tools
- Willingness and ability to obtain a US Government Top Secret Security Clearance
- Ability to complete projects independently, ensuring that finished work meets established standards for quality and timeliness
- Experience using proprietary and/or open source tools to gather and analyze intelligence

Preferred Qualifications:

- Foundational knowledge in information technology, to include hardware, networking, architecture, protocols, file systems and operating systems
- Foundational knowledge of multiple areas of cyber security operations, such as attack surface management, SOC operations, Intrusion Detection/Intrusion Prevention Systems (IDS/IPS), threats (including APT, insider, etc.), vulnerabilities, and exploits; incident response, investigations and remediation
- Experience with Analyst's Notebook and/or Palantir
- Experience with SIEM tools and technologies, such as ArcSight, EnVision, OSSIM and/or similar tools
- US Government Intelligence Community (IC) cyber experience
- Industry certifications in cyber security, such as CISSP, GSEC, and/or Sec+
- Industry certifications in networking, such as CCNA, CWNA and/or Net+
- Degree in a related field from an accredited program