Our company is growing rapidly and is searching for experienced candidates for the position of security cyber analyst. To join our growing team, please review the list of responsibilities and qualifications.

Responsibilities for security cyber analyst

- Train SOC analysts on IDS incident handling techniques
- Reviewing evidence of remediation of findings, providing guidance and expertise where necessary
- Submitting updates for existing system security plans based on POA&M closure or documented deviations from the implementation of security controls
- Interpreting policies, procedures, standards, guidelines, and regulations to include National Institute of Standards and Technology (NIST) and Federal Information Security Management Act
- Interpret, analyze, and execute incident response actions for detected intrusion anomalies and events
- Intercept and prevent internal and external cyber-attacks or attempts against PNNL systems
- Conduct system, network, and software vulnerability assessments and penetration testing
- Contribute to design, development and implementation of countermeasures of cyber security systems
- Collaboration with external entities including law enforcement, and other U.S. government agencies
- Partner with cyber security researchers on data analysis, prototype implementation, collaboration, and feedback

Qualifications for security cyber analyst

- Ability to anticipate and respond to changing priorities, and operate effectively in a dynamic demand-based environment, requiring extreme flexibility and responsiveness to business unit matters and needs
- Evening and weekend hours may be required
- Knowledge of networking protocols (such as TCP, UDP, DNS, FTP, SMTP, DHCP)
- Experience managing an investigation
- Bachelor's degree and at least 5 years' experience in a level 3 role
- Ability to gain and maintain a Public Trust