The job market for cyber security specialists is increasing at a rate of about 18 percent per year, according to the Bureau of Labor Statistics. That means if your company has a job to fill in this specialty, you’re competing against a lot of other firms.

## Cyber Security Specialist Job Description Template

We’re looking for a driven Cyber Security Specialist passionate about building innovating solutions to prevent against an ever-expanding battery of cyberattacks. We’ll look to you to defend our critical information and computer networks from opportunistic hackers, and we’ll also depend on you to keep your thumb on the pulse of the IT security sphere so you can take appropriate measures to keep our business and platforms protected.

You’ll get the opportunity to develop, implement, communicate, monitor and maintain our cyber security program, including identifying critical systems and critical digital assets, addressing cyber security controls for each critical digital asset, and maintaining cyber security attack mitigation and incident response capability.

Job Responsibilities:

* Provide security monitoring and incident response services required by the business, in alignment with Cyber Security’s mission to protect Client’s Digital Assets (including Industrial Control Systems) to a level of confidentiality, integrity and availability commensurate with the threat to those assets and their value to Client.
* Act as internal expert on matters relating to intrusion detection and incident response.
* Lead investigations into network intrusions and other cyber security breaches.Provide a coordinated response to complex cyber-attacks that threaten company’s assets, intellectual property, and computer systems.
* Contribute to the development and improvement of security monitoring and incident response processes and solutions as required to support our cyber security program.
* Operate security monitoring and incident response toolsets with a focus on continuous improvement.
* Research and recommend solutions for incident response and digital forensics.

Job Skills & Qualifications:

Preferred:

* 2 to 5 years of related experience in Cyber Security
* GCIA, GCIH and CISSP (or equivalent) certification (preferred)

Requirements:

* Experience in information security, specifically with penetration testing, intrusion detection, incident response or digital forensics
* Experience coordinating complex response activities with IT services department
* Experience working within a global team setting
* Bachelor’s degree in information security or in a related field