# Cyber Intelligence Analyst Career Overview**Job title:** Cyber Intelligence Officer

|  |  |
| --- | --- |
| **Job title:** | Cyber intelligence officers gather information about where threats to information technology (IT) systems come from and how they work. |
| **Routes and Entry requirements:** | **University**  You can do a degree or postgraduate qualification in one of the following subjects:   * computer science * computer or cyber security * mathematics * network engineering and security   You could take a postgraduate course in computing or cyber security if your first degree is not in a related subject, or if you have a lot of industry experience.  You'll usually need:   * 2 to 3 A levels, or equivalent, for a degree * a degree in a relevant subject for postgraduate study   **Apprenticeship**  You could do a higher or degree apprenticeship in:   * cyber security * cyber intrusion * network engineering   You'll usually need:   * 4 or 5 GCSEs at grades 9 to 4 (A\* to C) and A levels, or equivalent, for a higher or degree apprenticeship   **Work**  You could start work with an IT security firm, for example as a support technician after doing GCSEs or A levels, then work your way up while studying for further qualifications on the job.  **Other routes**  If you have a degree or relevant work experience, you could apply for [MI5's Intelligence and Data Analyst Development Programme](https://www.mi5.gov.uk/careers/opportunities/intelligence-and-data-analyst-development-programme-idadp). |
| **Skills required:** | You'll need:   * knowledge of computer operating systems, hardware and software * complex problem-solving skills * the ability to use your initiative * the ability to accept criticism and work well under pressure * telecommunications knowledge * to be thorough and pay attention to detail * persistence and determination * maths skills * to have a thorough understanding of computer systems and applications |
| **What you'll do:** | In this role you'll often be:   * identifying common weaknesses in IT networks * using digital resources to gather information and evidence * using computer forensics to identify attackers, their motivations and techniques * analysing threats to major security systems * monitoring new and evolving threats and assessing their potential impact * keeping databases of threats and hackers * producing threat assessment reports with recommendations for protective action * developing relationships with other organisations to safely share security knowledge * updating your skills and knowledge   Restrictions and requirements  For public sector work, you may need to go through UK Security Vetting. This includes:  a counter terrorist check  a security check (SC) - for access to information classified as 'secret'  developed vetting (DV) - for access to information classified as 'top secret'  For private sector work, you may not need to be vetted unless you're working on government systems. |
| **What you’ll earn:** | £31,500 Starter *to* £50,000 Experienced |
| **Working hours, patterns and environment:** | * Typical hours 35 to 40 a week * You could work evenings/weekends * You could work in an office or at a client's business. |
| **Career path and progression:** | With experience, you could become a specialised cyber security lead and then head of cyber security. You could also work as a freelance security contractor. |