Model job description

Malware analyst

Scope, purpose and nature of rôle

The primary function is to deal effectively and efficiently with actual or suspected malware infections, for instance investigating, stopping, resolving and helping to prevent a recurrence of malware incidents. This is a technical rôle requiring strong technical competence (*e.g*. reverse-engineering malware samples and running tests and simulations in strictly controlled lab environments). The analyst's secondary function is to assist in the design and implementation of malware controls, drawing on the experience of actual incidents and near-misses and knowledge of the malware situation at large plus the skills gained in connection with handling malware incidents. In the event of major incidents, the analyst is anticipated to offer competent technical support under considerable duress as part of the incident management and business continuity activities.

Distinguishing characteristics of the ideal candidate

The following personal characteristics are high on our wish-list:

- **Decisive**: able to make difficult decisions, prioritize and take appropriate action without prevaricating or unduly delaying, yet willing to be held to account for those decisions and actions, and willing to seek and accept advice from further subject matter experts where necessary;
- **Supportive** of work colleagues working under stress, as well as being cool, calm and collected;
- **Strong technical focus**: interested in and competent to explore the specific techniques used by malware to exploit technical vulnerabilities in IT systems and networks, as well as the social engineering techniques to exploit IT users.

Relevant qualifications, skills and experience

The following qualifications and experience are considered relevant and desirable for this rôle:

- **IT security:** a degree or equivalent, preferably with significant IT security content; GIAC GREM, Mandiant Advanced Malware Analyst or similar technical malware courses and qualifications; at least 2 years work experience in the field; ideally some exposure to ISO27k and ITIL;
- **Malware technologies:** substantial experience in dealing with malware, to the level of Windows internals, reverse engineering and assembly language. Prior employment in an antivirus company or in a similar malware analyst position is a definite plus point, but other technical rôles such as programming, network intrusion analysis *etc*. may be equally beneficial;
- **Incident management and business continuity:** some exposure to and ideally involvement in incident management and/or planning, preparing and exercising for business continuity;
- **Technical writing:** reporting on malware identified and analyzed is a routine part of the job.

Candidates must be willing to undergo background checks to verify their character, claimed qualifications and experience.

For more information

Contact Information Security or HR for more about this rôle and the recruitment process.