

## **Position: Security Incident Handler - Manila, Philippines**

Access' Security Incident Handler, Manila, Philippines, will be responsible for manning Access Tech's 24 x 7 x 365 Digital Security Helpline, providing rapid response information security capability to meet the needs of NGO staff, and other civil society clients around the globe.

We are looking for dedicated and passionate individuals whom possess much of the technical criteria outlined below, but more importantly, candidates are passionate about digital security, human rights, and personal liberties and are inspired by our mission to defend these rights and fight for open and secure communications for all. A successful candidate is someone who is always looking for ways to learn and improve, and who is dedicated to applying their computer and technical skills to help those in need across Asia and the world.

### **Essential Duties & Responsibilities:**

- Perform incident rapid response duties via phone, email, and other communication channels. Perform client risk assessments. Give structured advice and recommendations as required, verbally and in written format.
- Document case history and maintain chain of evidence.
- Perform investigations and forensic analysis as required. Give security training to clients as required.
- Mitigate DDoS attacks, worm and virus outbreaks, and targeted attacks with trojans, rootkits, and other malware
- Defend the computer systems and web presence of clients.
- Security harden and patch systems, inc. MS Windows, Mac OS X, and Linux.
- Build and deploy blackout resilient technologies in the field.
- Operate, manage, fix, tune, and upgrade IDS sensors, and operate a SEIM to analyze complex attacks and generate reports.
- Build, manage, tune, fix, and upgrade circumvention server capacity.
- Perform systems administration tasks as required.
- Do software development work as required.
- Appear in court and present forensic evidence if required.

### **Education:**

- Must have a core computer science / technical competency (eg Comp Sci degree)
- Extensive training covering most of the 'Essential Duties & Responsibilities' (see above) will be provided to the successful candidate for this role. No specialist security education is required beyond that received in obtaining the computer science degree.

### **Required Knowledge & Skills:**

- Some exposure to Microsoft XP, Vista, 7, 8, Mac OSX, and Linux operating systems. Familiarity with Wifi, TCP/IP, SMTP, HTTP/S, TLS, PKI, VPN, VM, SSH, etc.

### **Additional Desired Technical Skills:**

- IDS, Cisco networking, Apache and IIS HTTPDs, Squid Proxy/Cache, Mailman, Postfix, Firewalls, TAILS, Web development, Perl, C, PHP, Javascript, Wireshark, MySQL.

### **Required Personal Qualities:**

- Unshakable integrity and personal ethics; dedicated, reliable and trustworthy, with a willingness to provide feedback and ask for assistance in challenging situations.
- Energetic and confident. Comfortable performing multifaceted projects in conjunction with routine activities. Must possess strong analytical capabilities, be resourceful and well organized with excellent verbal and written communication skills.
- Must be able to work in a high stress emergency environment that requires sustained focus; have an appetite for responsibility and perform careful, diligent work. Must be able to work unsupervised.
- Willing and ready to learn new things, be trained in incident handling and intrusion detection; and be willing to adhere to a strict procedural modus operandi as defined by Access.
- Be available for travel throughout the Asia region and beyond at short notice and for periods up to three months in length.
- Keep technical knowledge and skills up to date, and be willing to attend trainings and conferences as required by Access.

**Language Skills:**

- Candidates should have good ability in English and Mandarin Languages. Spanish, Mandarin, Arabic, or other languages an advantage.

**Location:** Manila, Philippines

**Commitment:** Full-time, 8 hour daytime shift (business hours), 4 days on / 2 days off shift schedule.

**Remuneration:** TBD

**Reporting:** This role will report to the Security Incident Shift Lead – Manila, and Access' Technology Director.

**Application Requirements**

To apply, send a copy of your CV, a cover letter explaining your interest and qualifications for the position, and three references (only one may be academic) to: [jobs@accessnow.org](mailto:jobs@accessnow.org)

Please place “Security Incident Handler, Manila, Philippines - [Your Name]” as the subject line. Only applicants with a cover letter will be considered.