



Technical Equipment Maintenance Division, Ministry of Defence Defence Information Technology Unit (DITU)

**ENGINEER
VACANCY: 1**

SECTION / UNIT: DEFENCE INFORMATION TECHNOLOGY UNIT (DITU)

JOB DESCRIPTION (NOT LIMITED TO THE LIST BELOW):

- Responsible for providing technical expertise to related to cyber security controls such as security analysis.
- Formal reporting of results including written and presentation material.
- Implement cyber security related projects.
- Must possessed excellent verbal and written communications skills and a strong analytical mind.
- Evaluation of third-party leading-edge security products.
- Production and presentation of security material to peers and superiors.
- Must be willing to learn & share knowledge

REQUIRED TECHNICAL QUALIFICATIONS AND / OR EXPERIENCE:

- Must have one or more of the following skills:
 - A good understanding of Microsoft, Unix & Linux operating systems
 - Solid understanding of fundamental IT concepts such OSI Model; TCP states; SNMP; Proxy; SSH
 - IT Security Fundamentals (VLAN, IPSec, HTTP, DNS)
 - Wireless LAN Fundamentals
 - IT Networking (switches, routers)
 - Web Application Security (MySQL, Oracle, Postgres) and fundamental knowledge of SQL commands.
 - Understanding of Security Architectures (firewalls, IDS, encryption, protective monitoring, anti-malware)
 - Understanding of Vulnerability Assessment / Penetration Testing
 - Experience with basic scripting (Unix shell scripts, Perl, or Python)
 - Experience with network scanning software packages and devices
 - Experience with packet capturing software such as Wireshark, TCPDUMP.
 - Experience in log analysis and co-relation



SOFT SKILLS:

- Must be able to assess, triage and troubleshoot issues quickly and efficiently.
- Must have superior oral and written communication skills to facilitate assigned tasks.
- Ability to interact and communicate effectively within various levels of technical and management staff internally and with other sections.
- Must be a results-oriented team player
- Ability to learn new technologies very quickly with excellent troubleshooting and problem-solving skills
- Detail-oriented; Ability to work independently and as part of a team
- Ability to build positive working relationships with internal and external team.

MINIMUM EDUCATIONAL REQUIREMENTS:

- At least a bachelor's degree (Honours) in IT Security/Computer Security. Degrees in System or Software Engineering or Computer Science may be considered if Information Security skills can be demonstrated through work experience and/or Security Certifications (CEH, CompTIA Security+, etc)
- Subject areas of particular interest within the degree:
 - Operating Systems
 - Computer Systems Security
 - Cryptography and Information Assurance
 - Computer Systems & Internet technologies
 - Ethical Hacking
 - System Security and Administration



**Bahagian Pemeliharaan Kelengkapan Teknikal,
Kementerian Pertahanan
Unit Teknologi Maklumat Pertahanan**

JURUTERA

KEKOSONGAN: 1

SEKSYEN / UNIT: UNIT TEKNOLOGI MAKLUMAT PERTAHANAN (UTMP)

BIDANG TUGAS (TIDAK TERHAD KEPADA SENARAI DIBAWAH):

- Bertanggungjawab dalam memberikan kepakaran teknikal bagi perkara-perkara yang berkaitan dengan kawalan keselamatan siber seperti analisa keselamatan
- Menyediakan laporan analisa yang rasmi secara bertulis ataupun dengan mengendalikan taklimat
- Melaksanakan projek-projek keselamatan siber
- Mesti mempunyai kemahiran komunikasi secara lisan dan bertulis yang sangat baik dan minda analitik yang kuat
- Membuat penilaian ke atas produk-produk sekuriti yang terkini
- Menyediakan dan memberi taklimat bahan-bahan keselamatan untuk ahli unit dan pegawai atasan.
- Sentiasa bersedia untuk belajar dan berkongsi ilmu pengetahuan

KELAYAKAN DAN / ATAU PENGALAMAN TEKNIKAL YANG DIPERLUKAN:

- Sekurang-kurangnya memiliki kemahiran seperti berikut:
 - Kefahaman yang mendalam bagi *operating systems Microsoft, Unix dan Linux*
 - Pemahaman yang kukuh dalam konsep teknologi maklumat asas seperti *OSI model, TCP states, SNMP, Proxy SSH* dan lain-lain
 - Asas keselamatan teknologi maklumat (*VLAN, IPSec, HTTP/S, DNS*)
 - Asas *Wireless LAN*
 - Rangkaian teknologi maklumat (*switches, routers*)
 - Aplikasi keselamatan *web (MySQL, Oracle, Postgres)* dan pengetahuan asas *SQL commands*.
 - Pemahaman tentang *architecture* keselamatan (*firewalls, IDS, encryption, protective monitoring, anti-malware*)
 - Pemahaman tentang *Vulnerability Assessment/Penetration Testing*
 - Pengalaman dengan *scripting* asas (*Unix shell scripts, Perl* ataupun *Python*)
 - Pengalaman dengan pakej perisian dan peralatan *network scanning*
 - Pengalaman dengan perisian *packet capture* seperti *Wireshark, TCPDUMP* dan lain-lain



- Pengalaman dalam menganalisa *log* dan *co-relation*

KEMAHIRAN INSANIAH (SOFT SKILLS):

- Dapat membuat penilaian, *triage* dan penyelesaian isu-isu dengan cepat dan cekap
- Mesti mempunyai kemahiran komunikasi lisan dan bertulis yang baik untuk memudahkan pengurusan tugas-tugas yang diberikan
- Berkebolehan dalam berinteraksi dan berkomunikasi secara berkesan dengan kakitangan teknikal dan pengurusan dari pelbagai peringkat
- Mestilah seorang pemain pasukan yang *results-oriented*
- Dapat mempelajari dan mengikuti teknologi terkini dengan cepat serta mempunyai kemahiran penyelesaian masalah yang sangat baik
- *Detail-oriented*, dapat berkerja secara berseorangan mahupun secara berkumpulan
- Dapat membina hubungan kerja yang positif dengan kumpulan dalaman dan luaran

KELULUSAN AKADEMIK MINIMA:

- Sekurang-kurangnya mempunyai ijazah sarjana muda (*Honours*) dalam *IT Security/Computer Security*. Ijazah sarjana muda dalam *system engineering/software engineering/computer science* akan dipertimbangkan jika pemohon dapat menunjukkan kemahiran *information security* melalui pengalaman kerja dan/atau *security certifications (CEH, CompTIA Security+, dan lain-lain)*
- Bidang subjek yang diperlukan dalam kelulusan:
 - *Operating Systems*
 - *Computer Systems Security*
 - *Cryptography and Information Assurance*
 - *Computer Systems & Internet technologies*
 - *Ethical Hacking*
 - *System Security and Administration*