Analist FORENSIC securitate cibernetică

Nivel carieră: middle (2 - 5 ani)
Adresa jobului: Bucureşti
Limba engleză, cel puţin nivel mediu

Candidatul ideal

Studii superioare în domenii tehnice, preferabil informatică, automatică, electronică, matematică sau cibernetică, cu abilități pentru dezvoltarea de aplicaţii software.

Cunoştinţe aprofundate de lucru pe sisteme de operare (Linux, Windows și Mac OS)

Cunoştinţe generale:

- cunoştinţe privind **protocoale de comunicații** (*TCP/IP, HTTP, DNS, SMTP, FTP etc.*) și al infrastructurii unei rețele locale de calculatoare;
- cunoştinţe despre **sistemele de fişiere**: NTFS, FAT, EXT, XFS etc.;
- cunoştinţe despre **medii de virtualizare** (*VMWare, VirtualBox, KVM, ESX etc.*);
- cunoștințe cu privire la modul de investigare al incidentelor de securitate cibernetică;
- cunoștințe despre evaluarea vulnerabilităților și amenințărilor de securitate cibernetică;
- cunoştinţe cu privire la metodele și instrumentele folosite în domeniul Digital Forensics (*soluții software / soluții hardware*);
- cunoştinţe despre procesul de recuperare a datelor şterse/deteriorate de pe mediile de stocare;
- cunoştinţe despre modalitățile de stocare folosite în arhitecturile de tip server (RAID0, RAID1, RAID5, RAID6 etc.).

Cunoştinţe în unul sau mai multe din domeniile (avantaj)

- deținerea unor certificări tehnice valide în domeniul de specializare (EnCE, GCFA, GCFE, CompTia, CISCO etc.);
- Linux bash scripting, Python, Perl etc.;
- analiza log-urilor de pe sistemele de calcul (Linux, Windows, Mac OS);
- competențe cu privire la extragerea și analiza artefactelor dintr-o imagine a memoriei RAM;
- abilitatea de învățare și adaptare rapidă.

Descrierea job-ului

- investigarea incidentelor de securitate cibernetică din diferite infrastructuri;
- obținerea datelor și informațiilor relevante pentru investigarea atacurilor cibernetice;
- efectuarea unui analize tehnice cu privire la modul în care s-a produs atacul cibernetic (*factorii care au dus la producerea incidentului / tehnicile folosite de atacator etc.*)
- dezvoltarea, actualizarea și menținerea în stare de funcționare a sistemelor folosite pentru realizarea investigațiilor cibernetice.

Cum aplici?
Completezi acest **FORMULAR**.