



---

## Analist FORENSIC securitate cibernetică

**Nivel carieră:** middle (2 - 5 ani)

**Adresa jobului:** București

**Limba engleză,** cel puțin nivel mediu

### Candidatul ideal

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

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

#### Cunoștințe generale:

- cunoștințe privind **protocoale de comunicații** (*TCP/IP, HTTP, DNS, SMTP, FTP etc.*) și al infrastructurii unei rețele locale de calculatoare;
- cunoștințe despre **sistemele de fișiere:** NTFS, FAT, EXT, XFS etc.;
- cunoștințe 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;
- cunoștințe cu privire la metodele și instrumentele folosite în domeniul Digital Forensics (*soluții software / soluții hardware*);
- cunoștințe despre procesul de recuperare a datelor șterse/deteriorate de pe mediile de stocare;
- cunoștințe despre modalitățile de stocare folosite în arhitecturile de tip server (RAID0, RAID1, RAID5, RAID6 etc.).

#### Cunoștințe 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 cibernetică;
- 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 cibernetică.

### Cum aplici?

CV și scrisoare de intenție pe [hr.tehnic@sri.ro](mailto:hr.tehnic@sri.ro)