**Fișa de Post Securitate**

**Evaluat de st. gr. SI-201: Cebotari Dan**

**Analist malware**

**Domeniul de aplicare, scopul și natura rolului**

Funcția principală este de a trata eficient și eficient infecțiile cu malware reale sau suspectate, de exemplu, investigarea, oprirea și ajutarea la rezolvarea incidentelor malware. Acesta este un rol tehnic care necesită o competență tehnică puternică (de exemplu, inginerie inversă a mostrelor de programe malware și efectuarea de teste și simulări în medii de laborator strict controlate). Funcția secundară a analistului este de a asista la proiectarea și implementarea controalelor malware, bazându-se pe experiența incidentelor reale și aproape de erori și cunoștințele despre situația malware în general, plus abilitățile dobândite în legătură cu gestionarea incidentelor malware.

**Caracteristici distinctive ale candidatului ideal**

Următoarele caracteristici personale sunt importante pe lista noastră de dorințe:

• **Decisiv:** capabil să ia decizii dificile, să prioritizeze și să ia măsurile adecvate fără a afecta sau a întârzia în mod nejustificat, totuși dispus să fie tras la răspundere pentru acele decizii și acțiuni și dispus să caute și să accepte sfaturi de la alți experți în domeniu, acolo unde este necesar;

• **Susține** colegii de muncă care lucrează în condiții de stres, precum și să fie cool, calmi și liniștiți;

• **Focalizare tehnică puternică:** interesat și competent să exploreze tehnicile specifice utilizate de malware pentru a exploata vulnerabilitățile tehnice din sistemele și rețelele IT, precum și tehnicile de inginerie socială pentru exploatarea utilizatorilor IT.

**Calificări, abilități și experiență relevante**

Următoarele calificări și experiență sunt considerate relevante și de dorit pentru acest rol:

• **Securitate IT:** o diplomă sau echivalent, de preferință cu conținut semnificativ de securitate IT; GIAC GREM, Mandiant Advanced Malware Analyst sau cursuri și calificări tehnice similare pentru malware; minim 2 ani experienta in munca; în mod ideal, o expunere la ISO27k și ITIL;

• **Tehnologii malware:** experiență substanțială în tratarea malware-ului, până la nivelul elementelor interne Windows, inginerie inversă și limbaj de asamblare. Angajarea anterioară într-o companie de antivirus sau într-o poziție similară de analist de malware este un avantaj clar, dar alte roluri tehnice, cum ar fi programarea, analiza intruziunilor în rețea etc. pot fi la fel de benefice;

• **Scriere tehnică:** necesară pentru a raporta malware-ul identificat și analizat.

Candidații trebuie să fie dispuși să fie supuși verificărilor antecedentelor pentru a-și verifica caracterul, calificările și experiența pretinse.

**Îndatoriri și responsabilități**

* Serviți ca punct de contact principal pentru toate întrebările legate de malware;
* Analizați potențiale mostre de malware folosind o varietate de instrumente și tehnici;
* Dezvoltați și mențineți o înțelegere aprofundată a amenințărilor malware actuale;
* Identificați noi familii și variante de malware și actualizați semnăturile de detectare în consecință;
* Scrieți rapoarte cuprinzătoare care detaliază constatările și recomandările;
* Lucrați îndeaproape cu alți membri ai echipei de securitate pentru a asigura răspunsuri în timp util și eficiente la incidente;
* Fiți la curent cu cele mai recente tendințe și evoluții din industrie;
* Asistență la dezvoltarea și implementarea strategiilor de prevenire și răspuns a programelor malware;
* Efectuați revizuiri regulate ale sistemelor și rețelelor pentru posibile vulnerabilități;
* Efectuați audituri periodice ale software-ului și configurațiilor anti-malware;
* Instruiți personalul cu privire la gestionarea corectă a incidentelor de malware și contramăsurile adecvate;
* Menține documentația la zi a tuturor procedurilor.