



Summer Internship – Security Researcher

Cyber Threat Intelligence Team

Cluj-Napoca

Descrierea rolului:

Identificare continua de familii/atacuri noi si construire de euristici pentru identificarea de familii de malware si atacuri noi.

Responsabilitati

Threat Hunt: Monitorizare si identificare de familii si atacuri noi aparute pe fisiere de diferite tipuri (executabile, documente, scripturi etc).

Reverse engineering pe fisiere malitioase.

Imbunatatirea detectiei statice bazata pe continutul fisierelor (pentru diverse atacuri).

Clusterizare si imbunatatire detectie pe colectia de sample-uri malware deja existenta.

Imbunatatirea regulilor din sistemele de detectie automata.

Rezolvat tickete support tehnic pentru clienti/parteneri - probleme legate de detectie.

Cerinte

Cunoasterea unui limbaj de programare

Cunostinte despre arhitectura sistemelor de operare

Skilluri analitice/rezolvare probleme

Proiectele anterioare in domeniul securitatii cibernetice reprezinta un plus

Atentia la detalii