Analyst in Digital Forensics & Incident Response (Contract Agent Function Group IV)

CERT for the European Union Institutions, Bodies and Agencies

2020-07-13

Description of organisation & role

The CERT for the European Union institutions, bodies and agencies (CERT-EU) is looking to hire an Analyst to join its Digital Forensics & Incident Response (DFIR) team.

CERT-EU's mission is to act the cybersecurity information exchange and incident response coordination hub for over 60 constituents spread across the European Union. It is a respected member of the cybersecurity community, working closely with national and governmental CERTs/CSIRTs, other international organisations like NATO and a wide range of industry partners.

The primary purpose of this role is to contribute to the operations assigned to the DFIR team. It is a unique opportunity to further develop hands-on experience in the full spectrum of security activities, be exposed to complex incidents related to Advanced Persistent Threat actors and gain insights into the evolving threat landscape in an international, collaborative environment.

Main Responsibilities

The main responsibilities of the Analyst will include:

- Monitoring incoming communication (functional mailbox, emergency phone, various chats, and alerts in TheHive);
- Dispatching communications unrelated to security incidents to other teams in CERT-EU;
- Handling communications with CERT-EU peers and partners, including organizations such as the European Government CERTs Group (EGC), the CSIRTs Network (CNW), FIRST, TF-CSIRT, etc.;
- Triaging alerts and notifications related to incidents, vulnerabilities, or other threats;
- Reviewing alerts generated by specific tools, such as Splunk or IDS;
- Verifying vulnerability reports;
- Performing deeper analysis of detected incidents and alerts using the data available to CERT-EU (logs, infrastructure information, etc.) and open sources;
- Managing communication related to incidents with constituents;
- Assisting in drafting advisories and white-papers;
- Documenting and improving processes and procedures.

Essential qualifications, skills and experience

Graduate positions (such as the CA function group IV) require at least that you have completed university education (of three years).

The successful candidate will possess experience in IT Security with knowledge of some of the following domains:

- Vulnerability assessments and penetration testing;
- Knowledge of Windows, Linux, and MacOS operating systems;
- Log management tools for network log analysis (Splunk specifically is a plus);
- Tools for packet capture and analysis such as Wireshark or tcpdump;
- Web security including understanding of the underlying protocols;
- Static artefact analysis including debugging, code de-obfuscation, and reverse engineering basics;

- Scripting experience with special interest in JavaScript, Python, and PowerShell;
- Using and configuring sandboxes such as Cuckoo, FireEye, etc.;
- Memory forensics tools such as Volatility;
- Disk forensics tools, such as EnCase, FTK, the SleuthKit, or RegRipper;
- Cyber-threat intelligence sharing and in particular the MISP sharing platform;
- Experience in incident management tools, such as TheHive.

The candidate should also demonstrate the following skills:

- High level of customer-orientation and willingness to remain aware of customers' needs;
- Strong analytical and problem solving skills including the ability to deal with a large amount of information in a limited time;
- Ability to establish and maintain effective working relations with co-workers in an international and multi-disciplinary work environment;
- High degree of commitment and flexibility;
- Excellent communication skills in English, both orally and in writing.

Desirable qualifications, skills and experience

The ideal candidate will possess some, or all, of the following:

- Work experience in a complex public sector environment;
- General security certifications (e.g., CISSP);
- Certification in a Project Management methodology (e.g. PMI, Prince2) and/or in service management (e.g. ITIL);
- Experience in delivering trainings and public presentations.