Bitdefender

# Summer Internship – Security Researcher

ATC Detection Team

Cluj-Napoca

## Secure what matters along with Bitdefender

Bitdefender provides cybersecurity solutions with leading security efficacy, performance and ease of use to small, medium and large businesses and consumers. Guided by a vision to be the world's most trusted cybersecurity solutions provider, Bitdefender is committed to defending organizations and individuals around the globe against cyberattacks to transform and improve their digital experience.

We value initiative, diligence, innovation, commitment, enthusiasm and courage. Joining the Bitdefender team means building and maintaining a secure future for our customers in a fast-evolving threat landscape.

## The team and the project

This position is part of our Active Threat Control team, located in Cluj-Napoca.

Bitdefender Active Threat Control (ATC) is a proactive, dynamic detection technology, based on monitoring processes' behavior, and tagging suspect activities. It serves as a last line of defense against unknown malware. The ATC solution is built using the latest system monitoring technologies available on Windows. Using both User and Kernel Mode components, ATC is able to reliably monitor the behavior of running applications. The behavior is evaluated using an extensible heuristic engine.

The project also has an exploit detection module, a detection component based on machine learning and an attack research division.

You will be part of a friendly team whose mission is to tackle the challenges of real time detection to protect millions of users and to ensure customer satisfaction exercise their creativity with various research topics to improve the detection and our processes design and implement high quality software for current and future modules.

## Role:

Your mission will be to learn as much as possible, familiarize yourself with the working environment and the development processes, and use your skills to contribute to the efforts of the team.

Bitdefender

Responsibilities

Learn about process behavior monitoring techniques and technologies on Windows

Learn how and perform static and dynamic reverse engineering of malicious programs

Learn about exploitation and post exploitation methodologies

Learn how to define malicious process activity and create heuristics to detect it

Develop tests for existing and new heuristics

Develop C++ code that runs in User or Kernel mode (for Windows) inside Bitdefender behavioral detection components

Learn how to analyze market feedback to identify malware campaigns and false positives

Adjust existing detections to reduce false positives

Technical skills and expertise

Must have:

- Experience with programming in C or C++ (good understanding of pointers and memory management, working with files and processes, etc.)
- Understanding of data structures (trees, lists, hash tables, advanced searching algorithms, etc.)
- Ability to read and understand x86 Assembly

Nice to have:

- Familiarity with Windows API, system calls and concepts (such as HANDLEs, Windows processes, Windows threads, working with the Windows Registry)
- Experience with Assembly programming for x86 and AMD64
- Ability to use source level and Assembly level debugger (WinDbg, OllyDbg, Immunity Debugger or Visual Studio Debugger)
- Familiarity with operating system internals for Windows or Linux
- Knowledge about Windows PE format and how programs are loaded and executed
- Basic static reverse engineering skills (using IDA, GHIDRA, ILSpy) and/or experience with dynamic reverse engineering (using Procmon or Pin)
- Familiarity with network analysis tools (Wireshark)
- Familiarity with pentesting tools (Metasploit, PowerShell Empire, etc.)
- Participations to Capture The Flag competitions

Bitdefender

## Desired competencies and profile

Analytical & problem-solving skills

Interpersonal and team-oriented skills

Verbal and written communication skills

Self-motivated and enthusiast

Fast learner

## If you take up our offer, you will:

Be a member of a professional, motivated and enthusiastic team

Work on a project with a very important role in the Bitdefender products

Get a feel for how things are done in the cybersecurity industry

Learn skills that will greatly benefit your career

Enjoy a competitive salary, as well as medical and accident insurance

Make the world better by helping Bitdefender customers stay protected against cyber threats