## Contact

george.cabau@gmail.com

www.linkedin.com/in/george-cabau-0b77b371 (LinkedIn)


## Top Skills

Adaptation
Strategic Planning
Penetration Testing

## Languages

Romanian (Native or Bilingual)
English (Professional Working)

## Publications

Malware classification based on dynamic behavior
Multi-centroid cluster analysis in malware research
A new string distance for computing binary code similarities
Malware classification using filesystem footprints
From plagiarism to malware detection

# George Cabau


Director, Sandbox Technology at Bitdefender
Cluj, Romania


## Summary


With over a decade of experience in the cybersecurity field, I have cultivated a diverse skill set encompassing malware analysis, technical leadership, project management, and strategic planning. Beginning as a Malware Researcher, I honed my expertise in dissecting malicious software and identifying emerging threats. Progressing through roles such as Team Leader and Technical Project Manager, I have led multidisciplinary teams in developing innovative cybersecurity solutions, including sandbox technologies, attribution systems, network detection, and IoT vulnerability research. In my current role as Director of Sandbox Technology, I oversee the strategic direction and operational execution of initiatives aimed at combating evolving cyber threats. My blend of technical acumen and managerial prowess enables me to drive innovation, foster collaboration, and ensure the resilience of our digital infrastructure in the face of complex security challenges.


## Experience

### Bitdefender
15 years 6 months

#### Director, Sandbox Technology
February 2024 - Present (8 months)

Currently, as the Director of Sandbox Technology, I am entrusted with the strategic direction and operational oversight of our organization's sandboxing initiatives. I coordinate multiple teams specialized in developing cutting-edge sandbox technologies for detonating malware samples, refining attribution systems to identify malicious file authors, enhancing network detection capabilities, and conducting IoT vulnerability research. By leveraging my technical expertise and leadership skills, I steer our teams towards pioneering advancements in cybersecurity, safeguarding against emerging threats and ensuring the resilience of our digital infrastructure.

#### Senior Manager
January 2018 - February 2024 (6 years 2 months)

In this role, I assumed broader responsibilities encompassing both technical leadership and managerial oversight. I led multiple teams dedicated to the advancement of cybersecurity technologies, including sandbox technology development, attribution system refinement, network detection enhancement and IoT vulnerability research. Through strategic planning and resource allocation, I fostered a culture of innovation and collaboration, driving the teams towards achieving their goals and delivering impactful solutions that are part of our core detection systems, Bitdefender Box, Bitdefender GravityZone and other security solutions.

### Technical Project Manager
October 2014 - January 2018 (3 years 4 months)

As a Technical Project Manager, I orchestrated the planning, execution, and delivery of cybersecurity projects with precision and efficiency. I liaised with cross-functional teams to define project scopes, allocate resources, and manage timelines effectively. Through strategic project management, I ensured the successful development and implementation of sandboxing technologies, attribution systems, network detection solutions, and created a IoT vulnerability research team.

### Team Leader Malware Researcher
April 2011 - October 2014 (3 years 7 months)

Transitioning into a leadership role, I assumed responsibility for guiding a team of talented researchers in analyzing and dissecting complex malware. I facilitated collaboration and knowledge sharing among team members, fostering a dynamic environment for continuous learning and innovation. Under my leadership, our team made significant strides in threat detection and mitigation, earning recognition for our contributions to the field.

### Malware Researcher
April 2009 - April 2011 (2 years 1 month)

As a Malware Researcher, I conducted in-depth analysis of malicious software to understand their behavior and characteristics. I developed expertise in identifying emerging threats and vulnerabilities, contributing to the enhancement of cybersecurity measures. My work involved reverse engineering malware samples to uncover their underlying mechanisms and patterns, creating signatures and developing systems that could generate generic detections on malicious files, laying the groundwork for innovative defensive strategies.

# Education

## Universitatea Tehnică din Cluj-Napoca

Master’s Degree, Computer Science · (2011 - 2012)

## Universitatea Tehnică din Cluj-Napoca

Engineer's degree, Computer Science · (2006 - 2010)