

Persian Language Cyber Threat Intelligence Researcher

Location: Tel Aviv area, Israel

Summary of Position:

Intel 471 is looking for skilled cyber threat researchers at different levels who can research and track Persian speaking cyber threat actors in the criminal underground. The ideal candidate would have a background in tracking cyber threat actors online and have experience in law enforcement, military or security services.

Duties & Responsibilities:

- Monitor the Persian language cyber criminal underground where Persian speaking cyber criminals congregate, chat and buy and sell tools.
- Research specific threat actors as part of a global team to determine the who, what, when, where, why and how.
- Produce written reports of research findings and work collaboratively to identify knowledge/information gaps.

Qualifications, skills, knowledge or experience:

- Experience with cyber security, cyber threat intelligence, ethical hacking or cyber investigations.
- Fluency in Persian (reading and writing) and good English (reading, writing and speaking). English reports would be written in this role before being released to customers after editing.
- Understanding of common hacking tools (exploits, malware etc) and terminology.
- Understanding of cyber threat research including the ability to perform behavioural analysis of malware (with a sandbox), research a domain name, analyse passive DNS etc.
- Good open source intelligence (OSINT) gathering skills.
- Solid understanding of operational security aspects of conducting cyber threat research online.

How to apply:

Please contact us via emailing websitecontact@intel471.com .

About Intel 471

Intel 471 is an actor-centric intelligence collection capability for the world's leading cyber threat intelligence teams. To read more about Intel 471, see <https://intel471.com> and <https://www.scmagazine.com/sc-lab-approved-one-year-later-intel-471/article/633822/> .