Cease & Desist

Ethos Use Case 3.3

ethos
risk services

Positive Outcome

Ethos Risk Services was able to gather information on the subject from several sites that alluded to the subject's family, friends, interests, activities, education, and other items that could help pinpoint where to find the subject.

This Ethos case investigation resulted in:

Case Sent to Government

Concern: Server Hacking

A company authorized us to conduct an investigation on an individual they believed was hacking their server. The client initially wanted Ethos to utilize a contact in the region the hacker was believed to be but Ethos suggested an in-house investigation to reduce costs. Ethos was provided with a name, approximate age, and a few IP addresses.

Actions Taken:

- With the information provided, an in-house investigation was conducted on the subject and Ethos was able to gather information on the subject's behavior and close contacts via social media efforts. Ethos was able to gather information on the subject's behavior and close contacts.
- Ethos was able to uncover additional Social Media profiles and though unable to verify that they belonged to the subject, these profiles contained similar information, contacts, and posted media. Similarities on the subject were found across several other sites as well.
- The investigators compiled the list of related Social Media profiles found on Facebook, Twitter, Instagram, Wikimedia, VKontakte, Github, Codepen, and YouTube. Github and Codepen both contained information on two projects in Javascript. Content found on the YouTube profile related to downloading pirated games and other software.

Bottom Line:

In-House Ethos investigators were able to gather many leads on the subject's identity and were then turned over to the government to shut down the hacker.