Associate Threat Researcher

Description

As an Associate Threat Researcher, you will join Fortraâ��s Managed Threat Intelligence group: a world-class threat intelligence team focused on generating actionable threat intelligence findings for clients of Fortra Managed Services. With a core focus on email-based threats, account takeover attacks, and other digital impersonation fraud such as counterfeiting, this role helps Fortra clients fully understand the nature of the threats targeting them and gives critical intelligence to help clients most effectively prioritize aspects of their defensive posture. WHAT YOU'LL DO Actively research a variety of cyber threats using technical analysis techniques, data analysis, and both open-source and deep/dark web intelligence gathering. Produce both long and short form finished intelligence products taking the form of threat reports, intelligence briefings, whitepapers, and RFI deliverables. Partner with Marketing and other content teams to translate intelligence findings into blog posts and other material demonstrating Fortraâ��s thought leadership. Perform cutting-edge research on BEC and other types of phishing attacks. Write intelligence alerts, threat reports, whitepapers, and blog posts based on research findings from the Fortraâ��s Threat Intelligence teams. Participate in a peer review process of intelligence deliverables by providing notes and constructive feedback. Analyze threats to identify novel adversary capabilities, tactics, techniques, and procedures. Conduct data analysis to identify notable trends and activity groups in email-delivered, Account Takeover, and Digital Impersonation activity across the cybercrime ecosystem. Monitor previously identified activity groups over time to track activity and evolution in their behavior. Engage with customers and internal stakeholders to conduct RFI intake briefings and communicate threat research findings. This will involve presenting findings to key stakeholders. Other duties as assigned. QUALIFICATIONS 5+ years in security operations, or 1-3 years in intelligence analysis or investigative journalism. Strong understanding of social engineering techniques, phishing threats, and digital impersonation tactics. Experience analyzing email-based threats, including familiarity with SMTP and email header analysis. Fluent in reading web-based scripting languages including HTML, PHP, and JavaScript. Able to effectively develop intelligence requirements to an RFI via interaction with stakeholders. Exceptional research skills using both OSINT and private threat data. Experience querying both relational and non-relational databases. Outstanding data analysis skills and experience with data analysis tools, including Microsoft Excel. Exceptionally strong analytical reasoning, problem solving, and decision-making skills. Exceptional ability to write reports communicating complex research findings to a broad audience. Able to effectively present analytical findings to a wide range of audiences Ability to work independently and effectively as part of a remote team with minimal supervision. Relentless curiosity and desire to self-develop in order to keep up with the evolving threat landscape. Intermediate scripting knowledge, and a passion for automating routine or repetitive tasks. Experience with querying MySQL, MSSQL, Athena, MongoDB, and ELK systems. Familiarity with web-application penetration testing principles. Note: this job is not a pen-testing role. Experience analyzing web traffic using Wireshark, developer tools, or other mechanisms. Experience DE obfuscating code to facilitate analysis. Please mention the word **ILLUMINATI** and tag RMjE3LjYxLjIzLjE2MQ== when applying to show you read the job post completely (#RMjE3LjYxLjIzLjE2MQ==). This is a beta feature to avoid spam applicants. Companies can search these words to find applicants that read this and see they're human.

Contacts

Hiring organization
Fortra

Job Location
Remote

Base Salary
$ 70000 - $ 110000

Date posted
June 2, 2024

Apply Now

Job listing via RemoteOK.com