Byte

https://www.byte.eco/job/23666/

Senior Security Research Engineer

Hiring organization
Referral Board

Job Location
Remote

Base Salary
$ 60000 - $ 110000

Date posted
June 2, 2024

Apply Now

Description

About the Team: The Elastic Security Endpoint Protections team researches, designs, and builds visibility and detection capabilities that are integrated into Elastic Defend, our endpoint and SIEM security product. We are looking for a Senior Security Research Engineer to join our team and continue to innovate new features that will help secure our users against the latest emerging threats. You will collaborate with the broader Elastic Security team, which consists of a diverse group of skilled researchers, data scientists, and developers who possess extensive domain expertise in their respective areas. Our geographically dispersed team values positivity and inclusion in the workplace, collaborative learning, and candid communication. If you are passionate about security research and would enjoy the challenge of devising novel methods for thwarting malicious actors in an ever-evolving threat landscape, we would love to have you join our growing team! What You Will Be Doing: Research emerging attacker techniques and develop innovative and effective detection methods. Integrate additional visibility capabilities into our endpoint. Enhance preventions and detections over time to ensure we are staying ahead of the curve and improving efficacy. Develop code in a collaborative environment with peers in multiple countries and timezones. Monitor customer telemetry for false positives and establish appropriate mitigation strategies. Be active in the security research community through conference presentations and content published to Elastic Security Labs. Contribute to open source Elastic projects used by organizations around the world. Investigate security problems at scale with our global community of users. What You Will Bring Along: 5+ years of proven experience analyzing, studying, and understanding attacker tactics, techniques, and procedures (TTPs), as well as developing new methods and approaches for detecting advanced security threats using C, C++, and Python. In-depth reverse engineering and / or malware analysis experience. Verbose knowledge of Windows internals, core features, and system architecture. Collaborative mentality with a strong disposition to learn new skills and emerging technologies. Motivation to succeed in a distributed, fast-paced, and autonomous work environment. Passion for protecting the worldâ??s data from attack! Bonus Points: Significant experience in Windows development. Enterprise application development experience. Red teaming Windows networks. Vulnerability research and exploit development. Please mention the word **RICH** 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

Job listing via RemoteOK.com