Threat Intelligence Collection Manager

Us

Ensighten is a global cybersecurity leader, offering next generation client-side protection against data loss, ad injection and intrusion. Through the Ensighten solution, organizations can assess privacy risk and stop unauthorized leakage or theft of data, as well as comply with the CCPA, GDPR and other data privacy regulations. Ensighten's MarSec™ platform protects some of the largest brands in the world from data leakage whilst ensuring maximum web page performance.

The role

We are looking to hire a Threat Intelligence Collection Manager who will report into the Director of Threat Intelligence and play a part in the organization's threat intelligence capabilities.

The ideal candidate for this role will have a background in threat intelligence, will have strong communication and written skills, being able to collaborate internally, identify research gaps and opportunities, conduct planned and ad-hoc research and represent our intel internally, at conferences and for press opportunities.

The role will include the following responsibilities:

- Monitor the cybercriminal underground based off of ratio based keyword lists
- Create social network diagrams showing links between attacks and groups
- Keep up to date on new techniques used by Magecart communities
- Interact and create personas within Magecart or surrounding groups
- Input intelligence into collection platform

Key Requirements

- Extensive experience as a high performing practitioner in a cyber threat intelligence role
- Deep understanding and knowledge of the cybercriminal underground ecosystem and terminologies
- Subject matter expertise of common hacking tactics, techniques, and procedures (TTPs) such as malware, vulnerabilities, exploits, carding, fraud, etc
- Strong understanding of the interdependencies between cybercriminal enabling services, commodity products, compromised information/data, monetization schemes, and the threat actors involved
- Experience tracking malware, malware campaigns, phishing campaigns and infrastructure related to them
- Experience identifying and tracking TTPs commonly used for cybercrime and malware
- Proficient in open source intelligence (OSINT) research and common tool sets
- Knowledgeable of enterprise environments and teams, such as NOC, SOC, JOC, fraud, CTI, CISO groups, IT security; threat vectors and basic mitigating controls such as IPS, IDS, WAF, etc
- Experience leveraging knowledge to effectively articulate business risk with clients to enhance their cyber threat posture
- Passionate about protecting our customers across various industry verticals and capability levels

- Excellent time management and organization skills
- Excellent written and spoken communication, interpersonal, and problem-solving skills
- Must be a self-starter, motivated to take ownership and drive projects to completion

Location

There are no location requirements or stipulations for this role and the right person will be considered regardless of where they live. While travel is not part of the role, candidates must be able to occasionally travel for things such as company events.

Compensation

There is no defined compensation range for the role other than to say that we will be exceptionally competitive for the ideal candidate.

Education Requirements

There are no specific education requirements for the role – we are looking for the right person with the right abilities and the right mindset.

If you are highly motivated, we would love to hear from you. Please submit resume to careers@ensighten.com.