Job ID: 2018-0009

Sr. Cyber Threat Hunter

Job Summary

At Cysiv, we are building the future of cyber risk management as a service. Going above and beyond a traditional MSSP, we provide an advanced co-managed platform for detecting and responding to threats backed by enrichment, intelligence and data science. The Sr. Cyber Threat Hunter is a key member of the security operations team at Cysiv. This role is responsible for participating in threat actor-based investigations, creating new detection methodologies and providing expert support to the security monitoring/incident response team. The focus of the Threat Hunter is to detect, disrupt and eradicate threat actors from enterprise and cloud networks. To execute this mission, the Threat Hunter will use data analysis, threat intelligence, and cutting-edge security technologies.

Duties and Responsibilities:

- Hunt for and identify threat actor groups and their techniques, tools and processes
- Conduct Exploratory Data Analysis (EDA), including acquiring, engineering, and exploring various data types and log sources for detection opportunities
- Work with the detections engineering team to transform attacker TTPs into viable, low false-positive behavioral and signature detections using a variety of techniques including supervised, semi-supervised, and unsupervised ML, with an emphasis on sequential classification and pattern-matching
- Participate in "hunt missions" using threat intelligence, analysis of anomalous log data and results of brainstorming sessions to detect and eradicate threat actors on customer's networks
- Provide expert analytic investigative support of large scale and complex security incidents
- Perform analysis of security incidents for further enhancement of alert catalog
- Continuously improve processes for use across multiple detection sets for more efficient operations
- Document best practices using available collaboration tools and workspaces
- Communicate potential threats, suspicious/anomalous activity, malware, etc to the IR team, and be a point of contact to the customer
- Provide forensic analysis of network packet captures, DNS, proxy, Netflow, malware, host-based security and application logs, as well as logs from various types of security sensors
- Perform analysis of security incidents & threat actors for further enhancement of Detection Catalog and Hunt missions by leveraging the MITRE ATT&CK framework
- Provide support to SOC analysts as needed
- Validate suspicious events and incidents by using open-source and proprietary intelligence sources
- Document and manage incident cases in our case management system
- Interface with customers, as necessary, to resolve issues, provide additional information, and answer questions related to incidents and monitoring
- Keep up-to-date with information security news, techniques, and trends
- Become proficient with third-party threat intelligence tools as required

Requirements:

- Bachelor's degree or four or more years of work experience
- Four or more years of relevant work experience
- Experience as a SIEM Administrator
- Experience developing analytic queries using Elk
- Experience with Data Science Tools: Elasticsearch, Tableau, Kibana, Kafka

In addition, the ideal candidate will have:

- A master's degree in one of the following: Computer Science, Engineering, Mathematics, Business Intelligence, Statistics or Cyber Security
- CISSP, CISM or other security certification
- Experience normalizing and parsing large data sets
- Experience with open source tools to perform regression analysis
- Ability to independently perform statistical analysis and inference, data modeling, clustering and predictive analysis
- Ability to translate cyber and application security issues into analytical models. Capability to effectively multitask
- Excellent verbal and written communication skills
- Knowledge of security appliances and professional / open source tools that support threat hunting, including understanding the analysis of competing hypotheses
- Experience with either Red team or Blue team operations and ability to think both like an attacker and defender
- A passion for research, and uncovering the unknown about internet threats and threat actors
- The ability to successfully interface with both internal and external clients
- The ability to document and explain technical details in a concise, understandable manner
- The ability to manage and balance own time among multiple tasks, and lead junior staff when required

Location: U.S. or Canada, Remote

Cysiv provides equal employment opportunity for all applicants and employees. Cysiv does not unlawfully discriminate on the basis of race, color, religion, sex, pregnancy and childbirth or related medical conditions, national origin, ancestry, age, physical or mental disability, medical condition, family care leave status, veteran status, marital status, sexual orientation, or gender identity.