# Hunt Team Analyst

## Responsibilities

The Hunt Team Analyst provides incident detection and response services for our CyberDNA Managed Network Security Monitoring Service. This role performs proactive hunts to identify anomalous activity indicative of active compromise, previous compromise, misconfigurations, or other notable observations to support the protection of our customers' environments. When not hunting, this role triages and investigates alerts generated from multiple detection technologies & takes necessary action to identify, scope, and guide customers to a rapid and successful remediation.

As a contributor to the team, this role will spend up to 30% of its time broadening skills by

- participating in one-on-one hands-on mentoring with peers and senior team members
- researching new techniques for analysis & developing deeper technical analysis skills
- contributing to the security community through projects and presenting at conferences

while spending 70% or more heads down doing the mission:

- hands-on hunting, event triage & analysis across NSM sensors & managed endpoints
- consumption, analysis, and production of tactical threat intelligence
- development & maintenance of detection scripts, rules, signatures and related logic
- finding evil, and generally having fun kicking it out of places it shouldn't be

## Desired Qualifications

- 1-5+ years hands-on experience responding to cyber attacks
- Fundamental knowledge of common attack methods and their detection techniques.
- 1-2+ years experience doing Network Security Monitoring (NSM)
- Foundational knowledge of network traffic analysis, related tools
- 1-2+ years experience doing Host-based live response & analysis
- Experience deploying and using host based live response tools in multi-platform environments.
- Familiarity with malware analysis concepts and ability to perform basic static and dynamic analysis.
- 1-2+ years experience doing Event Log-based detection & analysis
- Skilled with log analysis tools, creating parsers, correlation rules, and managing dashboards.
- Basic scripting skills to pick up python, perl, or bash and automate analysis tasks if needed.
- Ability to learn & perform analysis quickly while balancing attention to detail and thoroughness.
- Strong interpersonal & communication skills working with remote peers over IM, phone & video.
- Ability to speak authoritatively and confidently while balancing respect & tact with customers.
- Customer focused, building first-name relationships and protecting their networks as your own.
- Experience providing managed NSM services to multiple customers is a plus.

## Other Requirements

- Ability to work independently with periodic guidance from senior analysts and leaders.
- Assist as necessary with the tuning of signatures, rules, alerts, parsers, and custom scripts.
- This role leverages a flex-schedule that may involve nontraditional working hours.
- Must be willing to participate in scheduled Watch rotations, and after-hours on-call as needed.
- Must be able to work from the Vigilant office (Cincinnati, OH) or remotely from a home office, depending on the candidate's skills and experience.
- This position is eligible to US citizens physically residing in the US, any offer of employment is contingent upon background, drug screen & reference checks.