THREAT HUNTER

FUNCTION: A threat hunter is inquisitive and adventurous, driven by an insatiable curiosity to explore the depths of digital realms and uncover hidden cyber threats. With a combination of strategic thinking, investigative skills, and technological expertise, the Threat Hunter navigates the cyber wilderness to proactively uncover and neutralize emerging cyber threats.

COMMON QUALIFICATIONS

- Ceaseless on-the-job training
- Self-study researching threats of interest
- Capture-the-Flag (CTF) competitions/exercises
- Deep understanding of operating systems and networking
- SANS certification
- MITRE ATT&CK knowledge
- DFIR experience
- Reverse engineering experience
- Blue Team experience
- Purple Team exercises
- Log analysis experience
- Other industry certifications

ABILITIES

Puzzle-Solving: Possessing a sharp and analytical mind, a Threat Hunter excels at connecting dots, spotting patterns, and deciphering complex cyber threats that lurk beneath the surface.

Digital Tracking: Skilled in tracking and tracing digital footprints left by threat actors, a Threat Hunter follows the trail of cyber threats to their source, uncovering hidden attack vectors and malicious activities.

Deep Log Analysis: Proficient in data analysis and correlation, a Threat Hunter sifts through large volumes of security data to identify patterns, anomalies, and potential indicators of compromise to spot the unusual outliers.

Collaborative Investigation: A Threat Hunter collaborates with SOC teams, threat intelligence analysts, and law enforcement agencies to conduct joint investigations and share threat intelligence.

Threat Analysis: They possess deep knowledge of malware, hacking techniques, and vulnerabilities, allowing them to quickly analyze threats, ranging from zero-day exploits to sophisticated phishing campaigns, and devise effective countermeasures.

> **"It's human nature to start taking things for granted again when danger isn't banging loudly on the door."**
>
> - David Hackworth

Proactive Hunting: Proficient in hypothesis-based threat hunting techniques, Threat Hunters formulate hypotheses about potential threats, gather evidence, and conduct thorough investigations to validate their suspicions.

Adaptive Strategies: Agile and adaptable, a Threat Hunter develops and implements innovative strategies and countermeasures to defend against evolving cyber threats on the fly.

Technical Acumen: A Threat Hunter's expertise in cybersecurity tools and techniques equips them with the skills needed to navigate intricate networks, query languages in different platforms, and identify potential vulnerabilities.

BINARY DEFENSE™

THREAT HUNTER

PERSONALITY TRAITS

Avid Researcher: On-the-clock or off-the-clock, a threat hunter is obsessed with studying emerging threats to be ready for them.

Analytically-Minded: Inquisitive nature, constantly asking probing questions and digging deeper into cyber threats, leaving no stone unturned in investigations.

Curious Explorer: Approaches threat hunting as a curious explorer, always seeking new challenges and discoveries within digital landscapes.

Creative: Learning a client's industry and environment, and then carefully crafting a hypothesis based on the threat model they are most worried about.

Driven: The hunt happens every day; a threat hunter is passionate about cyber and making clients safer, one hunt at a time.

Resourceful: Leverages technical skills and knowledge to devise creative solutions to complex cybersecurity challenges.

THREAT HUNTERS TEST AND SIMULATE KNOWN THREATS

A CURIOUS EXPLORER, ALWAYS SEEKING NEW CHALLENGES AND DISCOVERIES WITHIN DIGITAL LANDSCAPES

STANDARD EQUIPMENT

- In-house or home-based lab environments to entice threat actors in to watch their behaviors
- Access to massive amounts of data: leverage EDRs and SIEMs
- Static and dynamic malware analysis tools
- Reverse engineering tools
- Malicious samples to watch and see if there are any new behaviors and how they present themselves
- Threat Hunting Kit (digital forensics tools, network analysis software, threat intelligence feeds)
- Tactical Cyber Defense Manual (comprehensive guide to threat hunting techniques)

FIERCELY PROTECTING YOUR EVERYTHING

Meet all the Defenders at BinaryDefense.com

BINARY DEFENSE™

The Right Partner is the Best Defense