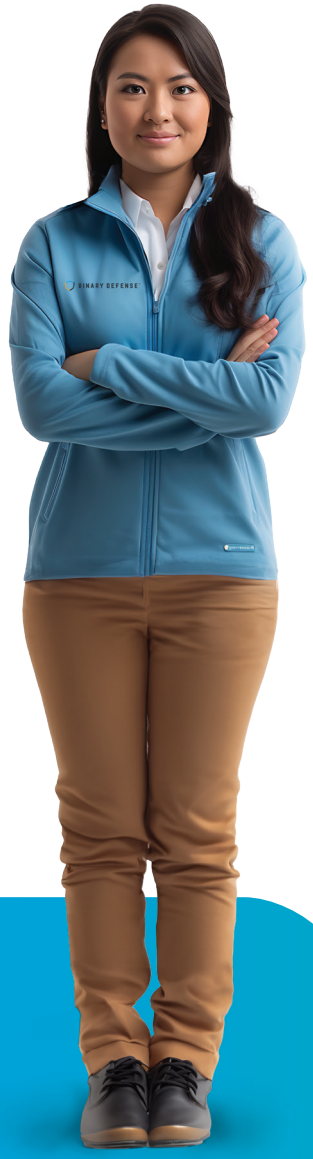
THREAT INTELLIGENCE ANALYST

FUNCTION: A Theat Intelligence Analyst not only understands threat actor tactics, but they also mimic them, hiding in the shadows of the dark web collecting information and turning it into valuable intelligence to share with fellow Threat Hunters, Analysts, and Researchers. Like a chameleon, a Threat Intelligence Analyst is fluent in the language and ways of criminal hackers, hostile nation state operators, and online transgressors, unraveling the threads of malicious intent to stay one step ahead of its mission and to better inform customers and prevent cyberattacks.

COMMON QUALIFICATIONS

- Curious, continual self-learner
- CompTIA: A+, Linux+, Network+, Security+
- AWS Solution Architecture and Azure Fundamentals
- Cyber Threat Intelligence certified (SANS)
- Network Forensic Analysis (SANS)
- Defending Against Advanced Threats (SANS)
- Certified Ethical Hacker (CEH)
- Other industry certifications



ABILITIES

Stealthy Investigations: Operating in the dark, a Threat Intel Analyst dons the guise of fake personas and navigates the intricate web of cyber threats with a keen eye and intuition to understand the intentions, behaviors, and motivations of cyber criminals.

Data Weaver: Like a weaver threading through a tapestry of digital threads, a Threat Intel Analyst culls through a variety of online sources, piecing together fragments of information and data patterns to unveil the hidden activities lurking in the shadows.

Shadow Lexicon Master: Possesses specialized skills to learn and understand the intricate vocabulary, slang, and cryptic terminology used by hackers in their communications, providing invaluable insight into their activities and intentions. They quickly grasp the nuances of hacker jargon, from obscure technical terms to colloquial expressions, deciphering the hidden meanings behind hackers' communications.

Technical Translator: Communication is a key trait. Recognizing the diverse backgrounds and levels of expertise among their audience, they tailor explanations to meet the needs of their audience, bridging the gap between technical jargon and layman's terms, ensuring that everyone can understand the risks associated with cyber threats.

"We constantly monitor the threat landscape, with the goal of identifying threats before they identify you."

Synthesis Savvy: Through careful observations, detailed research, or formal requests for information, a Threat Intel Analyst crafts compelling and informative written outputs – a threat watch on recent trends, a specific investigation request, a far-reaching customer-wide advisory, internal weekly reports, a media byline article, or a blog.

Chrono Insights: Possesses a deep understanding of historical data regarding cyber threats and the evolution of cybercriminal groups. By delving into the annals of digital history, they can effectively "time travel" through the cyber realms, unfolding the mysteries of past malware outbreaks and the rise and fall of nefarious organizations.

Global Understanding: Understands geopolitical and global issues that may fuel a cyber criminal enterprise.

BINARY DEFENSE™

THREAT INTELLIGENCE ANALYST

PERSONALITY TRAITS

Integrity: Having strong ethical standards is essential, as they are constantly confronted with sensitive data, and information. The very nature of their research involves understanding nefarious lucrative criminal tactics and abilities.

Critical Thinker: With a rigorous analytical mindset, a Threat Intel Analyst dissects data with precision, examining it from multiple angles and perspectives with an open mindset to eliminate any bias. They apply logical reasoning and deductive thinking to evaluate the validity and reliability of their findings; assess the potential risks and uncertainties associated with different scenarios, considering factors such as data quality, reliability, and potential biases.

Inquisitive Drive: With an insatiable thirst for knowledge and relentless pursuit of understanding, they have an innate curiosity that propels them to continually seek out new information, explore emerging technologies, and delve into the intricacies of cyber threats.

Persuasive Informant: Influences others with their wisdom and conviction of the importance of their findings, reaching out to clients and internal teams with compelling reports and insights.

Collaborative Aptitude: With a collective mindset, they recognize the importance of working effectively with others to achieve common objectives. They excel in teamwork, share knowledge, and contribute effectively, understanding the interconnected nature of cybersecurity operations.

Agile Prowess: A Threat Intel Analyst has a versatile skillset that allows them to seamlessly transition between tasks, from in-depth analysis to real-time incident response, reflecting their ability to swiftly adapt to the unpredictable nature of their role and switch focus as needed.

FOREWARNED IS FOREARMED

DOING OUR BEST TO HELP OUR CLIENTS AND TEAMS UNDERSTAND THE CURRENT THREAT LANDSCAPE

STANDARD EQUIPMENT

- Multiple accounts with different profiles to remain anonymous
- Insights from cyber underground and dark web forums
- Custom open-source intelligence (OSINT) Virtual Machines
- Additional intel feeds and dashboards
- Proprietary anomaly detection tools
- Programming tools and experience
- Website scanners
- File and URL analysis tools
- Automated malware analysis tools
- Network packet analyzers
- Camouflage / Hiding in Plain Sight (CTI)

FIERCELY PROTECTING YOUR EVERYTHING

Meet all the Defenders at BinaryDefense.com

BINARY DEFENSE™

The Right Partner is the Best Defense