DETECTION ENGINEER

FUNCTION: A Detection Engineer embodies the essence of a vigilant guardian of the digital wilderness, harnessing a deep passion for unraveling the intricacies of cyber threats through meticulous intelligence gathering, log analysis, and the art of crafting precise detection rules. They are the architects of modern defense techniques, leveraging their expertise in behavior analysis and pattern recognition to stay ahead of adversaries and protect digital ecosystems with dedicated precision.

COMMON QUALIFICATIONS

- SOC Analyst experience
- Sys / Net Admin experience
- Certified Information Systems Auditor (CISA)
- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- NIST Cybersecurity Framework (CSF)
- OffSec Certified Professional (OSCP)

ABILITIES

Investigative Enthusiast: Possesses an insatiable curiosity, constantly asking questions and delving deep into data to uncover anomalies and threats. Their analytical skills allow them to dissect complex information and extract meaningful insights.

Pattern Sleuth: With a keen eye for outliers and patterns, the Detection Engineer excels in detecting even the most subtle signs of cyber threats. They can differentiate between normal system behavior and malicious activities, ensuring accurate threat detection.

Log Whisperer: The ability to interpret log information with precision is a hallmark. They navigate through vast datasets, extracting meaningful information that informs the creation of detection rules tailored to the unique threat landscape.

Behavioral Analyst: Has an innate ability to decipher digital behaviors, recognizing subtle nuances that often evade traditional detection methods. They excel in dissecting behavioral patterns within log data and finding anomalies that signify potential security breaches.

Intel Collector: Avidly scours diverse intelligence sources, from threat feeds to open-source intelligence (OSINT), pulling actionable insights to fuel their detection rules.

Rule Artisan: Writing detection rules is both an art and a science for the Detection Engineer. They meticulously analyze historical attack data, conduct in-depth research on emerging threat tactics, and collaborate with threat intelligence teams to translate findings into effective detection strategies.

> **"Security is a process, not a product…The trick is to reduce your risk of exposure regardless of the products or patches."**
>
> - Bruce Schneier

BINARY DEFENSE™

DETECTION ENGINEER

PERSONALITY TRAITS

Analytical Acumen: With a sharp mind and keen analytical skills, they excel in breaking down complex problems into manageable components. They approach challenges with a methodical mindset, dissecting information to extract valuable insights.

Continuous Learner: Thrives on continuous learning and adaptation. They eagerly embrace new technologies, tactics, and threat trends, staying ahead of adversaries through constant improvement.

Tinkerer: Always tinkering with tools, scripts, and detection algorithms to enhance their effectiveness. They enjoy experimenting with new techniques and refining their craft through hands-on experience.

Collaborative Spirit: While capable of working independently, Detection Engineers understand the value of collaboration. They actively engage with cross-functional teams, sharing knowledge and insights to strengthen overall cybersecurity posture.

Strategic Thinker: Beyond technical expertise, they possess a strategic mindset. They can prioritize tasks, allocate resources effectively, and devise long-term cybersecurity strategies that align with organizational goals.

THEY EAGERLY EMBRACE NEW TECHNOLOGIES, TACTICS, AND THREAT TRENDS, STAYING AHEAD OF ADVERSARIES THROUGH CONSTANT IMPROVEMENT

THEY CAN DIFFERENTIATE BETWEEN NORMAL SYSTEM BEHAVIOR AND MALICIOUS ACTIVITIES, ENSURING ACCURATE THREAT DETECTION

STANDARD EQUIPMENT

- SIEM and SOAR Tools
- Data – to analyze
- Command line prompt – to gather and test detections
- Power shell scripts
- Sandbox – to simulate attacks before deploying to an environment
- Patience

FIERCELY PROTECTING YOUR EVERYTHING

Meet all the Defenders at BinaryDefense.com

BINARY DEFENSE™

The Right Partner is the Best Defense