# Tier 1 SOC Analyst

|  |  |
| --- | --- |
| Education | Bachelor’s degree (or equivalent) |
| Experience | 0-3 years’ experience with security operations or operating systems |
| Certifications | CompTIA certifications |

Tier 1 SOC analysts are the least experienced of the SOC team, responsible for initial analysis and triage of an incident. A Tier 1 analyst will be the first person to review each security event to determine if it is a false positive or potentially a security incident and will perform the initial data gathering and investigation of the event. If the event does appear to be a security incident, it will be escalated to the Tier 2 Responder.

# Tier 2 SOC Responder

|  |  |
| --- | --- |
| Education | Bachelor’s degree in a science (or equivalent); |
| Experience | 3-8 years’ experience including: incident response, threat mitigation, detection rule creation, operating systems, the MITRE ATT&CK Framework, Lockheed Cyber Kill-Chain, and packet analysis |
| Certifications | SANS Certifications such as GIAC Certified Incident Handler (GCIH), Cloud Forensics Responder (GCFR), and GIAC Certified Detection Analyst (GCDA). |

The Tier 2 analyst is more experienced than the Tier 1 and whose main job is to dig deeper in the incident that the Tier 1 has referred to them. The Tier 2 is the main responder to an incident and is responsible for identifying the root cause and to perform the incident response lifecycle.

# Tier 3 SOC Threat Hunting

|  |  |
| --- | --- |
| Education | Bachelor’s degree or higher |
| Experience | 7+ years’ experience in cybersecurity operations including (in addition to the Tier 2 skills) expertise in: scripting, network protocols, data analytics |
| Certifications | SANS GIAC Certified Incident Handler (GCIH) or Certified Threat Hunter (GCThH). |

The most experienced of the SOC staff, the threat hunting team is normally a smaller group that performs hunts into data sets looking for anomalies left by attackers that may have evaded the standard detection techniques.

# Forensics

|  |  |
| --- | --- |
| Education | Bachelor’s degree or higher |
| Experience | 4+ years’ experience in computer forensics |
| Certifications | Vendor specific certifications for EnCase, Cellebrite, X-Ways, or similar vendors. |

The Digital Forensics analyst is responsible for planning, organizing, collecting, processing, and analyzing bit-for-bit digital images of Windows and Linux platforms in the pursuit of an investigation.

# Malware Reverse Engineering

|  |  |
| --- | --- |
| Education | Bachelor’s degree or higher |
| Experience | 8+ years’ experience in malware reverse engineering |
| Certifications | GIAC Reverse Engineering Malware or IACRB Certified Reverse Engineering Analyst (CREA) |

The Reverse Engineer performs technical analysis of malicious binaries through controlled execution or static analysis of code and overcomes techniques designed to defeat analysis in order to identify functionality, capability, call-backs, and assist with the identification of indicators of compromise and possibly attribution.

# Threat Intelligence

|  |  |
| --- | --- |
| Education | Bachelor’s degree |
| Experience | 5+ years’ experience in cybersecurity, intelligence gathering, understanding the intelligence lifecycle (diamond model, etc.), understanding of adversary tactics and techniques, understanding of geopolitical landscape |
| Certifications | Certified Information Systems Security Professional (CISSP) or GIAC Cyber Threat Intelligence (GCTI). |

The Threat Intelligence team is responsible for conducting cyber research and analysis to identify external and internal cyber trends/observations as well as trends to highlight historical and present-day threat activities. The analyst will identify and analyze employed attacker Tactics, Techniques, and Procedures (TTPs) to support detections and response actions by the incident response teams to ensure full containment and eradication.

# Engineering Support

|  |  |
| --- | --- |
| Education | Bachelor’s degree in a science (or equivalent) |
| Experience | 2+ years’ experience in operating system administration, specific tool management, networking |
| Certifications | Operating system platforms or vendor specific tools required. |

The SOC engineering role is intended to support the tools necessary for the SOC to run. This would include things like the SIEM, IDS, and any endpoint solutions. This team would be responsible for both the tool maintenance as well as the configuration of such things like detection rules and access control.