A career as a Junior (Associate) Security Analyst

In the Junior Security Analyst role, you will be a Triage Specialist. You will spend a lot of time triaging or monitoring the event logs and alerts.

The responsibilities for a Junior Security Analyst or Tier 1 SOC Analyst include:

- Monitor and investigate the alerts (most of the time, it's a 24x7 SOC operations environment)
- Configure and manage the security tools
- Develop and implement basic IDS (Intrusion Detection System) signatures
- Participate in SOC working groups, meetings
- Create tickets and escalate the security incidents to the Tier 2 and Team Lead if needed

Required qualifications (most common):

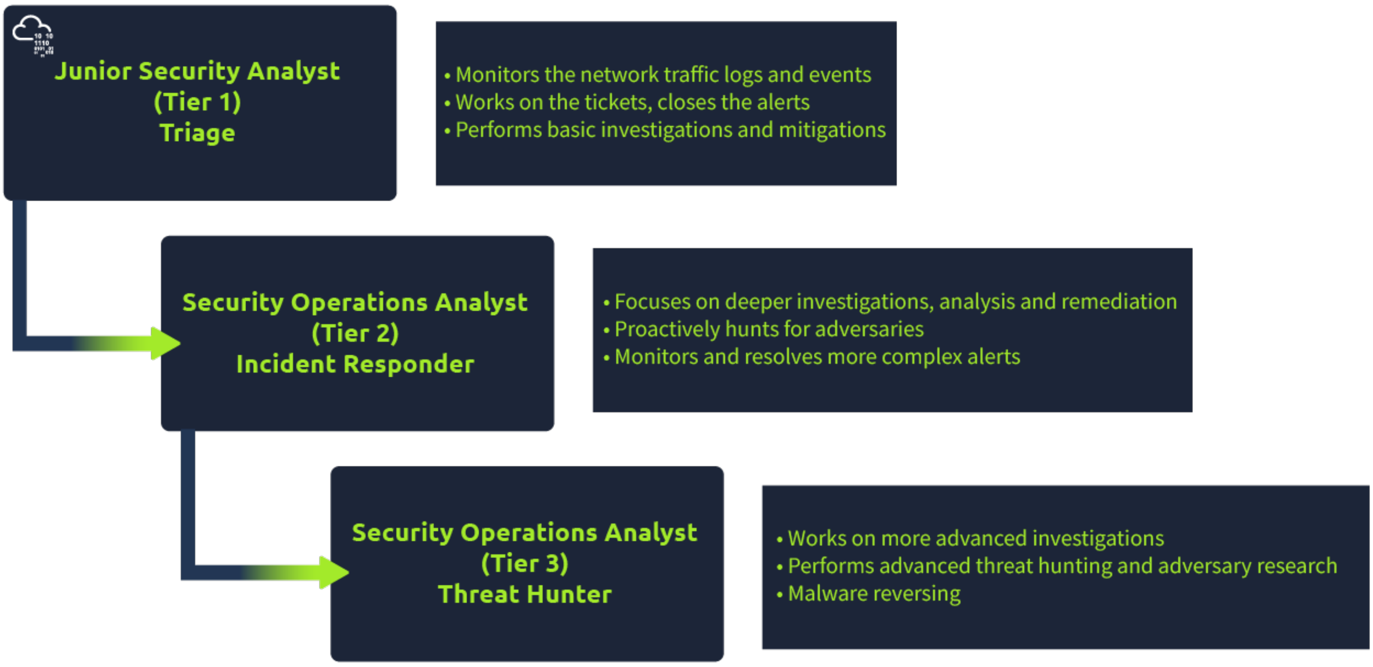
- 0-2 years of experience with Security Operations
- Basic understanding of Networking (OSI model (Open Systems Interconnection Model) or TCP/IP model (Transmission Control Protocol/Internet Protocol Model)), Operating Systems (Windows, Linux), Web applications. To further learn about OSI and TCP/IP models, please refer to the Introductory Networking Room.
- Scripting/programming skills are a plus

Desired certification:

- CompTIA Security+

As you progress and advance your skills as a Junior Security Analyst, you will eventually move up to Tier 2 and Tier 3.

An overview of the Security Operations Center (SOC) Three-Tier Model:


Junior Security Analyst
(Tier 1)
Triage
• Monitors the network traffic logs and events
• Works on the tickets, closes the alerts
• Performs basic investigations and mitigations
Security Operations Analyst
(Tier 2)
Incident Responder
• Focuses on deeper investigations, analysis and remediation
• Proactively hunts for adversaries
• Monitors and resolves more complex alerts
Security Operations Analyst
(Tier 3)
Threat Hunter
• Works on more advanced investigations
• Performs advanced threat hunting and adversary research
• Malware reversing

What will be your role as a Junior Security Analyst?

Revision #1
Created 19 January 2024 20:48:06 by naruzkurai
Updated 19 January 2024 20:59:40 by naruzkurai