A day In the life of a Junior (Associate) Security Analyst

To understand the job responsibilities for a Junior (Associate) Security Analyst, let us first show you what a day in the life of the Junior Security Analyst looks like and why this is an exciting career journey.

To be in the frontline is not always easy and can be very challenging as you will be working with various log sources from different tools that we will walk you through in this path. You will get a chance to monitor the network traffic, including IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) alerts, suspicious emails, extract the forensics data to analyze and detect the potential attacks, use open-source intelligence to help you make the appropriate decisions on the alerts.

One of the most exciting and rewarding things is when you are finished working on an incident and have managed to remediate the threat. Incident Response might take hours, days, or weeks; it all depends on the scale of the attack: did the attacker manage to exfiltrate the data? How much data does the attacker manage to exfiltrate? Did the attacker attempt to pivot into other hosts? There are many questions to ask and a lot of detection, containment, and remediation to do. We will walk you through some fundamental knowledge that every Junior (Associate) Security Analyst needs to know to become a successful Network Defender.

The first thing almost every Junior (Associate) Security Analyst does on their shift is to look at the tickets to see if any alerts got generated.

Are you ready to immerse yourself into the role of a Junior Security Analyst for a little bit?

Revision #1
Created 2024-01-19 20:55:48 UTC by naruzkurai
Updated 2024-01-19 20:59:40 UTC by naruzkurai