# **Readings: Log Analysis with Splunk**

1. What are three tasks which SOCs often perform?
   1. The three tasks that SOCs other performa are Incident Detection and Analysis, Incident Response and Mitigation, Threat Intelligence Analysis and Integration.
2. Explain what a SIEM solution is and how the SOC utilizes it in non-technical terms.
   1. The SIEM is a program that collects a lot of information inside a company and makes it accessible and easily readable in one place. The SOC utilizes it to maintain a company’s security or if something happens, they can easily find out what happened because of SIEM.
3. How does the typical SOC team structure resemble the structure of an IT Help Desk?
   1. The typical SOC team resembles the structure of an IT help desk because the goal of both jobs is similar, for example both are the first line of defense in case a security issue appears, in case it appears both have to do an incident triage and documentation for the incident.