

شرکت APK جهت استخدام کارشناس مانیتورینگ و تریاژ SOC از دانشجویان سماتک دعوت به همکاری می نماید.

### کارشناس مانیتورینگ و تریاژ SOC:

- پایش و رصد مستمر به صورت شناسایی حوادث امنیتی
- تریاژ و تحلیل اولیه رخدادها و حوادث امنیتی
- جمع آوری داده های لازم به منظور Escalate کردن هشدارها به لایه 2 مرکز SOC
- پاسخ اولیه به حوادث امنیتی
- مانیتورینگ سلامت سنسورها و زیرساخت سرویس دهی SIEM
- ارائه گزارش های دوره و موردی

دانش مورد نیاز:

- آشنایی با حملات شبکه ای، سیستمی و تحت وب
- آشنایی با یکی از پلتفرم های SIEM
- آشنایی با بدافزارها و تکنیک های مورد استفاده آنها
- آشنایی با Platform Mitre ATT&CK
- حداقل یک سال سابقه کاری مرتبط
- نوع همکاری: شیفتی و حضوری
- تهران
- حقوق بین 12 تا 18

متقاضیان محترم می توانند رزومه خود را با ذکر عنوان شغلی، به آدرس زیر ارسال نمایند:

ایمیل: [hr@favakar.ir](mailto:hr@favakar.ir)