SEMATEC
IT Training Center

شرکت سنباد جهت استخدام کارشناس SOC از دانشجویان سماتک دعوت به همکاری می نماید.

کارشناس SOC:

- پایش Alert ها و Dashboard های موجود در سازمان
- پایش Dashboard ها و اطلاعات مربوط به وضعیت SIEM
- بررسی و پیگیری Incident ها و موارد مشکوک مشاهده شده
- همکاری کامل با تیم فنی در صورت نیاز به Investigation های عمیق
- مستندسازی و ارائه گزارشات فنی در رابطه با موارد مشکوک مشاهده شده
- تهیه سازی گزارشات مدیریتی روزانه و هفتگی در رابطه با وقایع اتفاق افتاده در طول شیفت
- بررسی وضعیت Log گیری از منابع مختلف
- Incident Handling مواردی که مطابق با Play Book های در نظر گرفته شده انجام پذیر است
- گزارش موارد False Positive و پیشنهاد درباره نحوه Tune کردن Use Case مربوطه

تخصص های مورد نیاز:

- آشنایی با آناتومی حملات
- آشنایی با سیستم عامل های Windows و Linux
- آشنایی با روش ها و ابزار های انتقال و جمع آوری Log مانند Rsyslog, Nxlog, Splunk UF, WEC و ...
- آشنایی با انواع Log مناسب با Security Monitoring
- آشنایی با Use Case هایی که برای تشخیص حملات معمول کاربرد دارند
- آشنایی با حداقل یک SIEM (ترجیحا Splunk)
- آشنایی با Mitre ATT&CK
- آشنایی با Regex

مدارک و شرایط عمومی مورد نیاز:

- مدرک کارشناسی در رشته های مرتبط با فناوری اطلاعات
- حداقل یک سال سابقه کار در زمینه امنیت

SEMATEC
IT Training Center

- حداکثر سن 30 سال
- مدرک سربازی (برای آقایان)
- مدرک مرتبط با حوزه امنیت از قبیل Sec 504، CEH، +Security، Splunk و... مزیت محصوب می شود.
- روحیه کار تیمی و تعامل مناسب و اخلاق محور با همکاران تیم امنیت و سایر تیم ها از الزامات مهم همکاری می باشد.

رنج حدودی حقوق:

- 15 تا 20 میلیون تومان بسته به میزان موفقیت در مصاحبه فنی و عمومی

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

ایمیل: security@sanbod.co