SEMATEC
IT Training Center

شرکت امن پردازان کویر جهت استخدام در 2 عنوان شغلی زیر از دانشجویان سماتک دعوت به همکاری می نماید.

کارشناس مانیتورینگ و تریاژ SOC:

- آشنایی با حملات شبکه ای، سیستمی و تحت وب
- آشنا با یکی از پلتفرم های SIEM مانند: ELK ، Splunk ، Log Rythm
- آشنایی با بدافزارها و تکنیک های مورد استفاده آن ها
- آشنایی با Platform MITRE ATT&CK
- حداقل یک سال سابقه کاری مرتبط
- نوع همکاری: شیفتی
- محل کار: تهران

شرح وظایف:

- 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 مرکزsoc
- پاسخ اولیه به حوادث امنیتی
- مانیتورینگ سلامت سنسورها و زیرساخت سرویس دهیSIEM
- ارائه گزارش های دوره ای و موردی

کارشناس خبره SOC:

- تسلط کامل بر حملات شبکه ای، سیستمی و تحت وب
- تحلیل اولیه بدافزارها و تکنیک های مورد استفاده آنها
- آشنایی کامل باPlatform MITRE ATT&CK
- آشنا با یکی از پلتفرم های SIEM مانند...,ELK, Splunk,LogRythm
- تحلیل ترافیک شبکه ای
- آشنا به مفاهیم SANS 503/504/555

SEMATEC
IT Training Center

- حداقل سه سال سابقه کاری مرتبط
- محل کار: تهران

شرح وظایف:

- ریشه یابی حملات سایبری و آلودگی به بدافزار
- پایش و رصد مستمر به صورت شناسایی حوادث امنیتی
- بررسی و تحلیل کامل حوادثی که از کارشناسان لایه 1 ارسال شده است.
- جمع آوری داده های لازم به تحلیل و بررسی جامع رخدادها و حوادث امنیتی
- تحلیل آسیب پذیری ها سازمان و ارائه راهکار
- پاسخ کوتاه مدت به حوادث امنیتی در زمان SLA تایید شده
- ارائه راهکار مناسب پاسخ به رخدادهای امنیتی
- شکار تهدیدات سایبری
- پیشنهاد و تعریف سناریوهای امنیتی در ابزار SIEM متناسب با فضای تهدیدات سایبری
- رصد فضای سایبری به منظور شناسایی تهدیدات بالقوه و بالفعل
- ارتباط موثر با تیم پاسخ به حملات سایبری
- ارائه گزارش های دوره ای و موردی

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

ایمیل: Job@apk-group.net