کارشناس مرکز عملیات امنیت SOC و مدیریت رخدادهای امنیتی

- ✓ زمان لازم برای انجام: **۳ روز**
- ✓ داوطلبان گرامی لطفاً پروژه زیر را با دقت خوانده و پاسخ خود را در سایت بارگذاری نمایید.
- ✓ حجم فایل ارسالی بایستی کمتر از ۵ مگابایت باشد و پاسخ را در یک فایل zip به نام خودتان قرارداده و بارگذاری نمایید.

لطفا برای موارد زیر ارائه‌ی ۱۵ الی ۲۰ دقیقه‌ای آماده نمایید:

۱- تشریح چند مورد حملات مشهور حوزه وب و پیشنهاد روش‌های مقابله با آنها در یک مرکز soc

۲- شناخت و تشریح چند پروتکل شبکه و حملات مشهور آن و پیشنهاد نحوه‌ی شناسایی در یک مرکز عملیات امنیت

۳- انواع بدافزارها و مکانیزم عملکرد سه بدافزار مشهور و پیشنهاد نحوه‌ی شناسایی در یک مرکز عملیات امنیت

۴- شناخت mitre attack و تشریح تاکتیک‌ها و چند نمونه تکنیک در آن و پیشنهاد نحوه‌ی استفاده از این چهارچوب در مرکز عملیات امنیت

۵- تشریح چهارچوب آسیب پذیری FIRST و پیشنهاد چگونگی استفاده از آن در مرکز soc

۶-تشریح و مقایسه تمام راهکارهای siem و امتیازبندی جهت پیاده‌سازی