**Face to Face Mistakes: Ernst and Young**

1. Deviating from the topic.
2. Focus on the job responsibilities and speak what they want to hear.
3. Communicating good with peers.
4. Do not showcase your other skills. Instead focus on the topics which can be related to job.
5. Be Relaxed, confident.
6. Don’t be Over smart. Don’t bring in extra detail to the question and miss the important point.
7. Don’t be all over the place take a processed approach.
8. Show your strong experience with tools in resume.
9. Grind out and remember the job description as your resume
10. Body language

**Important things learnt in interviews:**

1. Tell what you have done not what your team has done.

Others Job Responsibilities:

1. Person 1:
2. • Monitors and Responds to cyber security incidents  
   • Created Google Chrome plugin to speed response time,easley pivot on dats, and integrated it with Splunk. Ensured plugin was easily added to by each member of response team  
   • Provides feedback to other teams in security department based on past experiences while on Red Teams in order to create IOC's and better detection's  
   • Developed Splunk queries for automated threat hunting with the analytics team  
   • Provided adhoc training to SOC team members to allow them to become more effective analysts  
   • Investigates and triage s events based on severity.   
   • Provides recommendations on how to mitigate the threats.   
   • Performs incident response during major cybersecurity events.   
   • Provides guidance to field resources on how to properly remediate a threat.   
   • Works closely with other Cyber Defense Team (CDC) team members to improve tools, techniques, and procedures for CDC operation.   
   • Continuously improves documentation of work products and processes.   
   • Participates in red/blue team exercises.   
   • Performs security analysis or reporting utilizing Security Incident and Event Management (SIEM)   
   • Documents Security Operations Center (SOC) policies and run book (aka TTP) procedures for incident response.   
   • Documents root cause analysis and lessons learned.

**Job Description Breakdown:**

**Associate Cybersecurity Threat Engineer**

**Required Experience**

(SIEM) Splunk , SPL, SOC functionalities ,Incident Response Activities, Cyber threat Intelligence, Ticketing systems.

**Drilling Deep Questions:**

OSI Layers and basics of security

**WIPRO JOB BREAKDOWN:**

**\*Part of vulnerability assessment.**

**\*Managing the Splunk Architecture**

**Worked for a client through offsite**

**Performed SOC 1 and 2 analysis**

**Threat modeling**