****

**QUANTUM UNIVERSITY**

**Mandawar (22 Km Milestone), Roorkee – Dehradun Highway (NH 73)**

**ROORKEE – 247 662**

**NOTICE**

**Department of Training & Placements**

Dated: 31.05.2021

Security HQ will be conducting placement drive for B.TECH CSE/ BCA/MCA 2021 PASSOUT students of Quantum University, Roorkee.

Details are as follows.

|  |  |
| --- | --- |
| Company Name | Security HQ |
| Company Website | <https://www.securityhq.com/> |
| Requirement & Skills | Acknowledge, analyse and validate incidents triggered from correlated events through SIEM solution.  Acknowledge, analyse and validate incidents received through other reporting mechanisms such as email, phone calls, management directions, etc.  Collection of necessary logs that could help in the incident containment and security investigation.  Escalate validated and confirmed incidents to SOC Analyst.  Undertake first stages of false positive and false negative analysis.  Understand the structure and the meaning of logs from different log sources such as FW, IDS, Windows DC, Cisco appliances, AV and antimalware software, email security etc.  Understand the subject of Carbon Black alarms.  Open incidents in SecurityHQ (ITSM Platform) to report the alarms triggered or threats detected. Analyst should properly include for each incident on SecurityHQ all details related to the logs, alarms and other indicators identified in accordance with the intervention protocol of each client and the SLA.  Track and update incidents and requests based on client’s updates and analysis results.  Properly log client requests and change requests in SecurityHQ  Report infrastructure issues to the SecurityHQ support team.  Report false positive alarms from Carbon Black and LogRhythm to L2 analysts.  Generate weekly reports from LogRhythm platform and send it to L2 for review.  Other duties related to the position.  **Other Skills**  Certifications: CCNA  Should have knowledge in Linux and Windows  Good communication skills  Good analytical skills  Quick learner  Team player |
| Eligibility Criteria | B.TECH CSE/BCA/MCA 2021 Passout |
| Designation | Security Associate – SOC Monitoring |
| Package Offered | Negotiable depending on experience |
| Selection Procedure | Online |
| Job Location | Work from home in pandemic after that Pan India |
| Recruitment Date | After registration |
| Reporting Time | 9.00 AM |
| Venue | Online |