Role: Cyber Security
Location: Gurugram
Emp. Type: Full-Time

This position is part of the IT Security & Compliance Division within Aramco Asia IT team based in Aramco Asia India Office. The candidate will support Aramco Asia regional - cybersecurity daily operations, lead cybersecurity projects, and work with external partners such as Saudi Aramco to secure the infrastructure. Furthermore, the candidate will help to secure Aramco Asia digital transformation roadmap into cloud-first strategy.

Job Description:

- Engage in evaluations, proof-of-concept activities, design, build and implementation of cybersecurity solutions, specializing in network security (such as Network Access Control, Zero Trust Network Access (ZTNA), Secure
- Access Service Edge (SASE), IPS etc.), other perimeter protection tools with minimal supervision and guidance.
- Perform core operational cyber-security functions such as co-managing security controls ranging from endpoint security, email security, web security, data leakage prevention.
- Respond to security incidents and manage incident responses.
- Provide cloud security assessment and propose enhancements and solutions.
- Review existing and proposed system configurations and designs to ensure compliance with security controls and baselines.
- Participate in or conduct cyber-security assessments, and evaluate proposed changes, and/or execute action plans to enhance cyber-security resilience and risk mitigation.
- Design, implement, operate, and maintain security tools, threat cases, advance detection solutions with minimal supervision and guidance.
- Enhance cyber-security operations functions through process enhancements and stakeholder engagement.
- Lead enhancement of cyber-security functions through vendor/supplier identification, scope of work development, justification, contract review, contract negotiation and procurement engagement.
- Execute and communicate enhancement strategy of cyber-security functions using measured goals, proper tracking and reporting.
- Establish, maintain, and enforce procedures, guidelines and baselines related to security for the users and administration of IT systems.
- Collaborate with stakeholders from other IT functions for cyber gaps remediations efforts and provide security review consultations if required.
- Implement security and data protection solutions in the cloud
- Strong understanding of API management and application integration methodologies
- Support in raising cybersecurity maturity of the organization.
- Perform other miscellaneous duties as directed

Education and Experience Required:

- Bachelor's degree in the IT field/Related field.
- 9 years' experience in IT and/or cybersecurity field.
- At least 5 years' work experience at an information security service-company or cybersecurity department.
- Candidate should be able to handle the incident report activities end to end.
- Must have knowledge of Splunk, Netspoke, Microsoft Defender, Azure Security, Network Security fundamental on IPS, firewall is a plus.
- Proficient in SIEM and Log Management Solutions. – SOAR solutions recommended.
- Strong Knowledge of modern cloud technology components and deployment patterns
- Intermediate or Advanced GIAC certifications in any of Cyber Defense, Penetration Testing, and/or Digital Forensics & Incident Response domains preferred (examples: GPEN, GWAPT, GCIH).
- CISSP/equivalent professional certification and Cloud security certification is preferred (CCSP, CCSE, AZ 500, GCSA, CompTIA Cloud+ etc)
- Proficient in written and oral English.
- Knowledge with emerging technologies, such as intelligent automation, artificial intelligence (AI)/ machine learning (ML)
- Experience with Windows hardening is a plus
- Ability to implement automation using script or via automation platforms such as SOAR, Power Automate is preferred
- Proficient in both Windows and Unix/Linux operating system implementation and administration.