Title: Red Team Cyber Security Analyst

Job Req ID: 12918

Description:

Aramco energizes the world economy.

Aramco occupies a unique position in the global energy industry. We are the world's largest producer of hydrocarbons (oil and gas), with the lowest upstream carbon intensity of any major producer.

With our significant investment in technology and infrastructure, we strive to maximize the value of the energy we produce for the world along with a commitment to enhance Aramco's value to society.

Headquartered in the Kingdom of Saudi Arabia, and with offices around the world, we combine market discipline with a generations' spanning view of the future, born of our nine decades experience as responsible stewards of the Kingdom's vast hydrocarbon resources. This responsibility has driven us to deliver significant societal and economic benefits to not just the Kingdom, but also to a vast number of communities, economies, and countries that rely on the vital and reliable energy that we supply.

We are one of the most profitable companies in the world, as well as amongst the top five global companies by market capitalization.

Overview

We are seeking a Senior Red Team Expert to join the Information Security Compliance Division (ISCD) of Information Security Department (ISD).

The ISCD is responsible for ensuring compliance with the enterprise's information security policies & standards, regulatory requirements & contractual requirements for all entities, technical platforms and cybersecurity domains.

The Administrator is primarily responsible for ensuring the development and execution of the global cybersecurity compliance framework and process to ensure that required cybersecurity controls are implemented. The Administrator is also responsible for ensuring the development and execution of Red Team framework, process, and protocol to provide assurance on cybersecurity identification, protection, detection & response capabilities, and to verify readiness and effectiveness of implemented cybersecurity controls on people, process and technologies. This role monitors & reports on status of non-compliance to related enterprise's Cybersecurity governing documents, national cybersecurity regulations and Red Team Findings.

The Cybersecurity Specialist primary role is to conduct a comprehensive security assessment, including penetration testing, vulnerability assessments, social engineering, and simulating real-world attacks to evaluate the effectiveness of our organization's security measures.

Duties & Responsibilities

- Perform comprehensive security assessments, including penetration testing, vulnerability assessments, and social engineering, to identify potential vulnerabilities in company's infrastructure, systems, and applications.
- Develop and execute detailed red teaming strategies tailored to the specific challenges and risks faced by the oil and gas industry, testing the effectiveness of our security

controls in protecting critical assets.

- Collaborate with cross-functional teams, including operations, IT, and engineering, to identify and prioritize critical assets, systems, and applications for testing, with a focus on protecting operational technology (OT) environments.
- Provide guidance and mentorship to junior team members, offering technical expertise and promoting professional growth in the context of oil and gas cybersecurity.
- Generate detailed reports outlining findings, recommendations, and remediation strategies to improve the overall security posture of our oil and gas infrastructure.
- Stay up-to-date with the latest hacking techniques, threat landscape, and industry best practices specific to the oil and gas sector, anticipating and mitigating emerging cybersecurity risks.
- Work closely with stakeholders in the oil and gas company to communicate findings, explain technical concepts, and provide actionable recommendations for risk mitigation, considering the operational and business impact.
- Contribute to the development and enhancement of oil and gas industry-specific red team methodologies, tools, and frameworks to improve testing efficiency and effectiveness.
- Develop and maintain red team infrastructure - Conduct threat intelligence analysis - Participate in purple team exercises - Develop and deliver training on red teaming and offensive security
- Work independently and as part of a team, and be able to communicate effectively with both technical and non-technical audiences.

Minimum Requirements

- A Bachelors degree in Cybersecurity, Computer Science or equivalate degree from a recognized and approved program. An advanced degree in addition to CISSP and CISM certificates are preferred.
- Minimum 10 years of experience in Cybersecurity including knowledge in cybersecurity red teaming.
- You must have strong experience in conducting red team assessments, penetration testing, and vulnerability assessments.
- Proven track record of successfully identifying vulnerabilities and weaknesses in critical infrastructure, SCADA systems, and industrial control systems (ICS) is a requirement.
- Experience with network and application security testing in operational technology (OT) environment is a requirement.

- Familiarity with relevant cybersecurity standards and frameworks specific to the oil and gas industry, such as ISA/IEC 62443, NIST SP 800-82, and API RP 1164 is preferred.
- Experience leading and conducting red team engagements - Experience developing and executing complex attack scenarios - Experience using a variety of offensive security tools and techniques - Experience evading detection and responding to incidents is a requirement.
- You must have deep understanding of oil and gas industry processes, equipment, and technologies, including SCADA, DCS, RTUs, and PLCs.
- Using specialized tools and protocols relevant to oil and gas cybersecurity, such as Wireshark, Modbus, DNP3, and OPC is preferred.
- You must have strong knowledge of scripting languages (e.g., Python, PowerShell) for automation and tool development.
- Excellent problem-solving and analytical skills, with the ability to think creatively and strategically to address oil and gas security challenges is also necessary.
- Effective communication skills, both verbal and written, to convey complex technical concepts to non-technical stakeholders is a requirement.
- Strong project management skills, with the ability to prioritize tasks and meet deadlines in a dynamic environment is also a requirement.
- You must have experience with the MITRE ATT&CK framework - Experience with cloud security Experience with web application security - Experience with exploit development - Experience with reverse engineering

Working environment

Our high-performing employees are drawn by the challenging and rewarding professional, technical and industrial opportunities we offer, and are remunerated accordingly.

At Aramco, our people work on truly world-scale projects, supported by investment in capital and technology that is second to none. And because, as a global energy company, we are faced with addressing some of the world's biggest technical, logistical and environmental challenges, we invest heavily in talent development.

We have a proud history of educating and training our workforce over many decades.

Employees at all levels are encouraged to improve their sector-specific knowledge and competencies through our workforce development programs – one of the largest in the world.

Country/Region: SA