Indian Financial Technology & Allied Services

Job Description

I	Role Summary		Remarks
	(a) Title:	Security Analyst - Cyber Security	L1
	(b) Business/Function:	Cyber Security	
	(c) Band / Designation:	Security Analyst - Cyber Security	L1
	(d) Location:	Hyderabad/Mumbai	
	(e) Reports to:		
	(f) Team:	Cyber Security	
	(g) Summary:	Security Analyst will be supporting day to day Cyber Security Operations	
	(h) Position Code:		
II	Additional Information		
	(a) Responsibilities:	•Monitor and support 24x7 for Security Operations, which include detection, tracking and analyzing incident alerts and generating daily, weekly and monthly reports. •Operation support experience in SIEM solutions preferably on LogRhythm/QRadar. •Analysis, alert raising and monitoring of various dashboards in LogRhythm/QRadar. •Integration of various log sources to SIEM solution. •Deployment/Integration of an EDR solution in a large customer environment, preferably Checkpoint EDR •Perform the health check on day daily for various security tools and solutions. •Responsible active support on SIEM, SOAR, UEBA, NBAD,DLP,Proxy solutions. •Knowledge and Administration of VA PT tools and techniques. • Knowledge of information risk, governance and compliance concepts and principles. •Understand and follow Security process documents and SOPs for different SOC functions and solutions like IEM, SOC, VA, PT, WAF, NBAD, DLP. •Strong problem-solving skills to troubleshoot, be able to understand technically assigned tasks and create knowledge documents. •Good communication skills. Excellent in written and verbal communication.	
III	Requirements		Classification
	(a) Education:	BSC / Diploma in computer science with relevant experience in Information Security.	Mandatory
	(b) Experience:	1-3 years	
	(c) Certifications:	CompTIA Security+ , CEH, SIEM (IBM QRadar, LogRhythm, SPLUNK)- At least one is mandatory	Specified within
	(d) Knowledge:	•Experience in monitoring, research, assessment and analysis on alerts from various security tools, including SIEM, Anomaly detection systems, antivirus systems, user behavior analytics tools, endpoint inspection, and proxy devices. •Provide threat and vulnerability analysis as well as security advisory services. Analyse and respond to previously undisclosed software and hardware vulnerabilities. Investigate, document, and report on information security issues and emerging trends •Experience in performing VAPT for organization's assets and applications. •Knowledge in Cyber Security solutions & tools as well as must be aware of day-to-day attack coverage.	Specified within
	(e)Technical Skills:	Primary Mandatory Skills: Experience in SIEM, VA, PT , WAF, SOC, PIM Secondary Desirable Skills: Understanding of Firewall, Proxy, DLP, NBAD	Specified within