Indian Financial Technology & Allied Services			
Job Description			
I	**Role Summary**		Remarks
	(a) Title:	Senior Security Analyst - Cyber Security	L2
	(b) Business/Function:	Cyber Security	
	(c) Band / Designation:	Senior Security Analyst- Cyber Security	L2
	(d) Location:	Mumbai	
	(e) Reports to:	Manager	
	(f) Team:	Cyber Security	
	(g) Summary:	1) The candidate will be responsible for Cyber Security solutions of IFTAS. 2) The candidate will be supporting the security solutions.	
	(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. •Implementation and Operation support experience in PIM/PAM & IAM Solution. •Implementation and Operation support experience in SIEM solutions preferably on LogRhythm/QRadar. •Analysis, alert raising and monitoring of various dashboards in SIEM. •Integration of various log sources to SIEM solution. •Deployment of an EDR/XDR solution in a large customer environment. •Perform the health check on day daily for various security tools and solutions. •Leading the Cyber Incident response process to ensure timely triage, analysis, containment, eradication and return to service for high severity/ long running/Critical incidents. •Responsible for management, technology assessment, continuous improvement & other technical activities on security solutions and tools like Anti-malware/EDR/XDR, CDR, PIM, Proxy, Email GW, WAF, Firewall, SIEM, SOAR, UEBA, SOC, NBAD, DLP, DAM, MDM, IAM, & VAPT/Patching etc. •Responsible for ensuring adequate configurations, troubleshooting and the resolution RCA etc. of Cyber Security tools. •Blocking, managing, & monitoring the activities on WAF & DAM Solution. • Administration of Vulnerability Assessment tool & Penetration Testing. •Perform internal & external Penetration Tests, Application & Network vulnerability assessment scans, and security risk assessment reviews. •Manage vendor relationships for technical, design, projects and implementation. •Identify and detail information risk, governance and compliance concepts and principles. •Develop processes documents and SOPs for different security solutions and tools – Anti-malware/EDR/XDR, CDR, PIM, Proxy, Email GW, WAF, Firewall, SIEM, SOAR, UEBA, SOC, NBAD, DLP, DAM, MDM, IAM, & VAPT/Patching etc. •Strong problem-solving skills to troubleshoot, must be able to understand technically assigned tasks and create knowledge documents.	
III	**Requirements**		Classification
	(a) Education:	Graduation in any stream or Diploma in Engineering with relevant experience in IT Security / Cyber Security.	Mandatory
	(b) Experience:	4+ Years of relevant experience •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. •Ensure that the SOC team is performing its functions as required and to trouble shoot problematic incidents and events. •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 •Deployment & Operation Support in a large customer environment for security solutions and tools like - Anti-malware/EDR/XDR, CDR, PIM, Proxy, Email GW, WAF, Firewall, SIEM, SOAR, UEBA, SOC, NBAD, DLP, DAM, MDM, IAM, & VAPT/Patching etc. •Experience in performing VAPT for operations assets and applications. •Experience in PIM Operations, support and implementations preferably Arcon PIM.	Mandatory
	(c) Certifications:	CISM, CEH, CompTIA Security+, CySA+	Preferred
	(d) Knowledge:	1) Knowledge in Cyber Security solutions & tools as well as must be aware of day to day attack coverage.	Mandatory
	(e)Technical Skills:	Technical skill in configuring, troubleshooting and managing security solutions and tools like – Anti-malware/**EDR/XDR**, CDR, **PIM**, Proxy, Email GW, WAF, Firewall, SIEM, SOAR, UEBA, **SOC**, NBAD, DLP, DAM, MDM, IAM, & **VAPT**/Patching etc.	**Specified within**