File No. BECIL/GM(P)/PROJECT/02/Advt.2020 Dated: 27. 04. 2020

BROADCAST ENGINEERING CONSULTANTS INDIA LIMITED

(A Government of India Enterprise under Ministry of Information & Broadcasting)
(A Mini Ratna Company)
Head Office: BECIL, 14-B, Ring Road, Indraprastha Estate, New Delhi – 110 002
Phone: 011-23378823, **Fax**: 011-23379885
Corporate Office: BECIL Bhawan, C-56/A-17, Sector-62, Noida-201 307
Phone: 0120-4177850, **Fax:** 0120-4177879 **Website:** www.becil.com

Applications are invited for recruitment/ empanelment of following manpower purely on contract basis for deployment in Government offices New Delhi /Hyderabad through an authorized agency of BECIL.

S/N	Post	Requirement	Qualifications & Experience
1.	Cyber Crime Threat Intelligence Analyst (for Hyderabad)	01 (For **Hyderabad**)	Annexure-I
2.	Digital Forensic Expert	02(For **Delhi**)	
3.	Cyber Crime Investigator(s)/ Cyber Crime Investigation Researcher(s)	03 (For **Delhi)**	
4.	Software Developer(s)/ Software Programmer(s)	03 (For **Delhi)**	
5.	Content Developer	01(For **Delhi)**	

B.

S/N	Post	Requirement for Delhi	Level-1	Level-2	Qualifications & Experience
1.	Mobile Forensic Expert	12	07	05	Annexure-II
2.	Network Forensic Expert	02	01	01	
3.	Memory Forensic Expert	02	01	01	
4.	Malware Forensic Expert	08	04	04	
5.	Cloud Forensics Expert	04	02	02	
6.	Crypto Analysts	04	02	02	

C.

S/N	Post	Requirement for Delhi	Level-1	Level-2	Qualifications & Experience
1.	Data Analysts	02	01	01	Annexure-III
2.	Malware Researchers	01	01	00	
3.	Open Source Intelligence Professionals	04	02	02	
4.	Programme Manager	01	0	01	
5.	SME for Cyber Crime Investigation	01	0	01	

***Note: Number of vacancy may change.**

Only shortlisted CVs will be informed for interviews. Interviews will be held in Delhi. NO TA/DA will be paid for attending the interview. The interview will also include skill test on the IT Tools.

Interviews may be conducted in two steps if necessary. Online interviews may be conducted if required.

Candidates who have applied previously may do so again.

The CV and **prescribed proforma Annexure-IV (provided by BECIL)** may be sent on the email **cyberjobs@becil.com**.

Candidates applying for more than one post may use separate proforma for each post.
The candidates appearing for interview must carry a hardcopy of the CV along with ID proof and passport size photograph.

Last date for receipt of application is **06.05.2020**.

Sd/-
General Manager

Annexure-I

1. Job Description for Cybercrime Threat Intelligence Analyst

Total years of experience	Relevant years of experience	Number of position/s	Indicative monthly Professional fee (INR)
5+ years	More than 3 years	01	Rs.1,40,000/- per month

Key responsibilities and required skill sets

- Detect emerging Cybercrime threats based upon analysis, data feeds crime reporting and sources (internal & external intelligence sources). Working within the team and the wider Information Security group to build new tools for intelligence gathering.
- Building and maintaining senior management dashboards to provide a clear understanding of team activities and threat landscape.
- Using data from social media, open sources, search engines, public records, and the deep web to compile detailed reports on cybercrime, criminals and criminal infrastructure
- Review unlawful and suspicious content in open source and escalate violations to the appropriate govt. department
- Collect, organize, analyse and develop reliable actionable intelligence about cybercrime, criminals, criminal infrastructure from open sources
- Must have advanced understanding of how to use open-source including social media for intelligence.
- Proven ability to work both independently and as a team and present/develop ideas
- Ability to work effectively with technical and non-technical stakeholders.
- Ability to communicate (verbal and written) with stakeholders in non-technical terms.
- Experience with multiple social media platforms.
- Active Cyber Threat Hunting & provide recommendations to optimize cyber security based on threat hunting discoveries.
- Analyse and correlate incident data to develop a Perform Root cause analysis and suggest corrective actions and preventive actions.
- Identify and suggest appropriate infrastructure with suitable mitigation strategies for cyber crime
- Evaluate target systems to analyse results of scans, identify and recommend resolutions
- Producing periodic Cybercrime threat analysis reports with mitigation measures
- Scripting and programming skills with proficiency in one or more of the following; PowerShell, Pearl, Python, Javascript.
- Knowledge of computer and network forensics investigations, malware analysis.
- Knowledge of cryptographic protocols.
- Experience with security assessment tools, including Nmap, Nessus, Wireshark, Metasploit, Nexpose etc.
- Experience in other areas such as data loss protection, threat assessment, hunting and intelligence, access management, knowledge of VAPT

Essential qualification

- B.E/ B.Tech / Computer Science/ Electronics and communication; or
- Engineering Graduate / M.Tech ; or / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication
- Understanding of network protocols, data on the wire, covert channels, ciphers and shell scripting

Desired certification/s

- Industry certification like CISSP / CISM / CEH / OSCP / or any other equivalent certification
- Experience in working with Law Enforcement agencies in India or Abroad is desirable

2. Job Description for Digital Forensic Expert

Total years of experience	Relevant years of experience	Number of position/s	Indicative monthly Professional fee (INR)
5+ years	5 years	02	Rs.1,25,000/- per month

Key responsibilities and required skill sets:

Technical:

- Ability to identify the fundamental concepts and technologies involved in computer, digital devices and networking
- Knowledge of computer, mobile device, network, cloud and other wireless communication technologies
- Analysing the forensic data on a variety of conventional disks, phones/smart phones/cloud/memory, as well as having in- depth understanding of the limitations of existing methods for extracting data from the digital devices
- Examine the resources related to virtualization and various cloud storage applications or services.
- In-depth knowledge of investigations in virtual environments, cloud forensic models, architectures, chain of dependencies etc.
- Ability to independently evaluate multiple operating systems, network configurations, network architectures, and topologies for identifying attacks/vulnerabilities.
- Demonstrate in-depth knowledge of network capturing/assessing tools used to analyse traffic at the application layer, network layer, translating it to identify and interpret inconsistent/anomalous activity in packet details.
- Ability for capturing network data, collection, distribution, analysis and presentation.
- Ability to draft SoP/RFP/Advisory Manuals/Reports pertaining to cyber crime investigation & digital forensics.
- Ability to assist in in-house projects pertaining to Digital Forensic/Cyber Crime investigation tools & capabilities

Non-Technical:

- Project planning and execution of cyber research projects, Program/ Project implementation and management, outreach activities, designing and delivering training programs, project plan development, RFP proposal writing, Research designing & Report writing, Monitoring & Evaluation, Impact Evaluation, Communication & Presentation skills.

Experience:

- 5+ years of experience in Digital Forensic Examination (Disk Forensics, Mobile Forensics, Network and Cloud Forensics etc.)

Educational Qualifications:

- Bachelor in IT/ Computer Science/Electronics and Telecommunication; or Engineering Graduate/ M.Tech; or BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/Electronics and Telecommunication.
- **Desired industry certifications** like CHFI, GASF, GNFA, IACIS Certified Mobile Device Examiner (ICMDE), GCFA, GCIH, GIAC, ENCE CFE, or equivalent certification related to forensics domain

3. Job Description for Cyber Crime Investigator/ Cyber Crime Investigation Researcher:

Total years of experience	Relevant years of experience	Number of position/s	Indicative monthly Professional fee (INR)
5+ years	5 Years	03	Rs.1,00,000/- per month

Key responsibilities and required skill sets

- In depth experience with industry standard cyber security/digital forensic methodologies, including SOC/SIEM/PENTEST/VAPT/BUG-HUNTING/SECURITY AUDIT or Digital Evidence Handling, Chain of Custody procedures, and commonly used Digital Forensic Life Cycle.
- Excellent knowledge of digital hardware, computer programming, cyber security practices, experience in different file systems, database's & operating systems artefacts.
- Ability to work under limited supervision, work with different investigation teams to aid in investigation and to plan and execute forensic support for both simple and complex investigations.
- Knowledge of computer science and laws related to computer evidence recovery as well as

procedures for the collection, preservation and presentation of computer evidence.

- Examine artefacts related to cryptographic and various crypto storage applications or services.
- In-depth knowledge of investigations in encryption concepts, chain of dependencies etc. Perform analytics on crypto products like crypto-currencies using available tools as well as through developing bespoke tools.
- Monitor open source content including social media platforms and other web space to identify and report any cybercrime/ anti-national/ dangerous/ undesirable activities.
- Using data from social media, open sources, search engines, public records, and the deep web to compile detailed reports on cybercrime, criminals and criminal infrastructure
- Review unlawful and suspicious content in open source and escalate violations to the appropriate govt. department
- Responsible for co-ordinating with the social media platforms and other online platforms
- Collect, organize, analyse and develop reliable actionable intelligence about cybercrime, criminals, criminal infrastructure from open sources
- Information Security certification are a strong plus
- Must have advanced understanding of how to use open-source including social media for intelligence.
- Must have strong communication skills (verbal, written)
- Proven ability to work both independently and as a team and present/develop ideas
- Ability to work effectively with technical and non-technical business owners.
- Ability to communicate (verbal and written) with stakeholders in non-technical terms.
- Ability to clearly document and communicate findings, opinions, and recommendations to both technical and non-technical audiences.
- Ability to draft SoP's/ RFP/ Advisory Manuals/ Reports pertaining to cybercrime investigation & digital forensics.
- Ability to assist in in-house projects pertaining to Digital Forensic/ Cyber Crime investigation tools & capabilities development.

Experience:

- 5+ years of experience in Cyber Crime Investigation/Research or in the field of Cyber Security/ Digital Forensics/ Cyber Crime Investigation

Educational Qualifications:

- Bachelor in IT/Computer Science/Electronics and Telecommunication; or Engineering Graduate/ M.Tech; or BCA /MCA or any other post graduate degree in the area of IT/ Computer Science/Electronics and Telecommunication.
- **Desired industry certifications** like CEH, CHFI, OSCP, GCFA, GCIH, GIAC, ENCE CFE, or equivalent certification related to cyber security/forensics domain
- Industry certifications related to OSINT/ social media analytics/Cyber Defence/Information Assurance/Experience of working with open source social media based investigations.

4. Job Description for Software Developer/ Software Programmer:

Total years of experience	Relevant years of experience	Number of position/s	Indicative monthly Professional fee (INR)
5+ years	5 years	03	Rs.1,00,000/- per month

Key responsibilities:

- Design and development of Software/Applications.
- Possesses high level understanding in the areas of web application programming, mobile application development, content management systems, API, database and system design.
- Must have strong understanding of software engineering practices and have analytical ability along with quality approach to the software design and development.
- Excellent debugging and problem-solving skills.
- Ability to work independently as well as in teams with members.
- Ability to assist in in-house projects pertaining to Digital Forensic/ Cyber Crime investigation/Cyber Security tools & capabilities development
- Ability to draft SoP's/ RFP/ Advisory Manuals/Reports pertaining to cyber security, cyber crime investigation & digital forensics.

Technical Skill Sets:

- Knowledge of HTML, CSS, JavaScript, Jquery, Ajax, PHP
- Web technologies like .NET / J2EE etc.
- Databases like SQL Server / Oracle / Postgre SQL etc.
- Programming languages like VB / C# / JAVA / Python/ C++ etc

Experience:

- Minimum 5 years of post-qualification experience in Software Development.

Educational Qualification:

- Bachelor's degree in Engineering in Electronics & Communication/ Electronics & Instrumentation / Computer / Computer Science / Computer Science & Engineering/ Electrical & Electronics/ Electrical / Information Technology/ Information Science only

5. Job Description for Content Developer:

Total years of experience	Relevant years of experience	Number of position/s	Indicative monthly Professional fee (INR)
5+ years	5 years	01	Rs.1,00,000/- per month

Key responsibilities and required skill sets

- Help research key cyber investigation/forensic topics and convert it into problem statements
- Research and writes content for S0Ps, Guidelines, Manuals, Booklets and other best practices to be issued by the organization in English/Hindi.
- Writes content, engaging text, etc. which are also to host on the web
- Assists in updating material of the organization as and when necessary and curates the content
- Develop different types of content for diverse audiences
- Develop, Revise, edit, and proofread content as needed or directed
- Fluent in English both writing and typing is necessary.
- Assist in developing documentation to help streamline the work of others and increase consistency
- Outstanding writing and verbal communication skills
- Great interpersonal skills and the ability to engage with many internal/external groups
- Strong knowledge in MS-Office Suite

Experience:

- 5+ years of experience writing business content for a technical audience for a company and/or a Govt. organization
- Experience in Audit/Cyber Security/Software Development/EoI/RFP and other training content development experience
- Experience in MS-Office Suite

Educational Qualifications:

- Any degree from a recognized university with experience of Digital Forensic/ Auditing/ Security/ Investigation will be preferred

1. Name of the Profile: Mobile Forensic Expert

Number of Post: 12

A mobile forensic personnel will acquire the process of gathering information from mobile devices and associated media.

Description	Relevant years of Experience	Number of Position	Indicative monthly professional (INR)
Level 1	1-3 years	07	Rs.1,53,550
Level 2	More than 3 years	05	Rs. 2,31,300

Key responsibilities and required skill sets

- Ability to identify the fundamental concepts and technologies involved in mobile forensics
- Knowledge of mobile device wireless communication technologies
- Analysing the data on a variety of conventional phones/smart phones, as well as having in-depth understanding of the limitations of existing methods for extracting data from these devices.
- Ability to decode/query and extract the data from latest versions of popular file systems like android, iOS, Blackberry OS etc.,
- Ability to reverse engineer software packages
- Ability to write executive summary and detailed report writing of the analysed devices
- Demonstrated hands-on experience of proprietary and open source mobile forensic tools
- Ability to selectively eliminate irrelevant information and determine the proper tool for analysis
- Ability to extract data in advanced mobile forensic methods like chip-off, JTAG etc.
- Conducting forensic analysis combined with an ability to accurately record full documentation in support of the investigation
- Thorough understanding of standard evidence handling procedures
- Proficient with digital forensic techniques and the most commonly used computer forensic tools

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate / M. Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

- Industry certifications like GASF, IACIS Certified Mobile Device Examiner (ICMDE), CHFI or other equivalent certification

2. Name of the Profile: Network Forensic Expert

Number of Post: 02

A network forensic personnel will capture, analyse about network/Network events in order to identify attack source or other Incidents.

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	1-3 years	01	Rs.1,53,550
Level 2	More than 3 years	01	Rs. 2,31,300

Key responsibilities and required skill sets

- Ability to independently evaluate multiple operating systems, network configurations, network architectures, and topologies for identifying attacks/vulnerabilities.
- Demonstrate in-depth knowledge of network capturing/assessing tools used to analyse traffic at the application layer, network layer, translating it to identify and interpret inconsistent/anomalous activity in packet details.
- Ability for capturing network data, collection, distribution, analysis and presentation.
- Familiarity in data analysis and visualization.
- Ability to analyse log from multiple IT assets.
- Knowledge of common tools that can facilitate large-scale analysis and repeatable workflows and libraries that can be linked to custom tools and solutions
- Ability to establish and present a timeline of the attacker's activities.
- Develop planning and strategy for capturing packets from commercial and home-built platforms, devices.
- Provide capacity building trainings to employees to prevent, detect, or mitigate the same or similar attacks.
- Conducting forensic analysis combined with an ability to accurately record full documentation in support of the investigation
- Thorough understanding of standard evidence handling procedures
- Proficient with forensic techniques and the most commonly used computer forensic tools

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate / M. Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

- Industry certifications like GNFA, Network+, CCIE, CCNA, CHFI or other equivalent certification

3. Name of the profile: Memory Forensic Expert

Number of position/s: 2

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	1-3 years	01	Rs.1,53,550
Level 2	More than 3 years	01	Rs. 2,31,300

Key responsibilities and required skill sets

- The memory forensic expert will analyse computer's memory dump to investigate and identify artefacts of cybercrime. Memory forensic expert will provide visibility of the run time status of the system.
- Collect important artefacts like those relating to process running, disk encryption keys, chat records and active network connections.
- Perform memory forensics, analysis and extract IOCs (Indicators of Compromise)
- Document process, procedure and reports pertaining to incident detection and response related to memory.
- Ability to acquire memory/RAM from various OS (windows, Linux, Mac) and devices (desktops, Laptops, Tablets etc.)
- Ability to detect intrusions in real-time
- Ability to use standard memory forensic tools, including Encase, FTK, write blockers, disk imaging tools etc.
- Understanding of tools such as Volatility framework, Redline etc. for analysis of RAM dumps
- Understanding of process memory, event logs, Registry in memory.
- Ability to track user activity
- Ability to reconstruct events and timelines
- Evidence management and chain of custody to ensure that the continuity and integrity of evidences is preserved
- Provide regular briefings and updates to the management

- Conduct research into new tools and techniques to enhance memory analysis process
- Conducting forensic analysis combined with an ability to accurately record full documentation in support of the investigation
- Thorough understanding of standard evidence handling procedures
- Proficient with forensic techniques and the most commonly used computer forensic tools

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate / M. Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired qualification

- Industry certifications like GNFA, GCFA, CHFI or other industry equivalent certifications

4. Name of the profile: Malware Forensic Expert

Number of position/s: 8

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	1-3 years	04	Rs.1,53,550
Level 2	More than 3 years	04	Rs. 2,31,300

Key responsibilities and required skill sets

- Examine malicious software, such as virus, worms, Trojans etc. to understand their structure/ signature/ behaviour.
- In-depth knowledge of OS & Application software internals, capable of documenting the attack capabilities of the malwares, understand its propagation characteristics, and define/create signatures for detecting its presence.
- Ability to identify and classify malware families based on standard taxonomy
- Stay abreast with latest malware threats and recommend IT infrastructure to defend against them.
- Collect structured and unstructured data from enterprise file servers, email, database systems
- Utilizes understanding of attack signatures, tactics, techniques and procedures associated with advanced threats
- Analyse the attack/exploit capability of malware, document, and catalogue findings and Develop necessary procedures or scripts to identify such data in future.
- Analyse collected media for defensive cyber operations and understand adversary technical capabilities, Tactics, Techniques and Procedures (TTP) and methods of employment.
- Understanding of tools and technologies to identify zero day attacks.
- Present tactical and strategic intelligence about threat actors, methodologies, and motivations based on malware research and develop methods of tracking and detecting malicious activity within a network.
- Use various tools and techniques to analyse malicious document files, executables and web-based malware.
- Conducting forensic analysis combined with an ability to accurately record full documentation in support of the investigation
- Thorough understanding of standard evidence handling procedures
- Proficient with forensic techniques and the most commonly used computer forensic tools

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate / M. Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication
- Should have experience in performing security incident response and/or digital forensic analysis.

Desired certification/s

- Industry certifications like GCFA, CHFI, CEH, GREM, CISSP, GCFE, GNFA OSCP, OSEE, OSCE CREST or other equivalent certifications

5. Name of the profile: Cloud Forensics Expert

Number of position/s: 04

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	1-3 years	02	Rs.1,53,550
Level 2	More than 3 years	02	Rs. 2,31,300

Key responsibilities and required skill sets

- Examine artefacts related to virtualization and various cloud storage applications or services.
- In-depth knowledge of investigations in virtual environments, cloud forensic models, Architectures, chain of dependencies etc.
- Ability to acquire data remnants from Dropbox, SkyDrive, Google Drive etc.
- Ability to identify evidence source and its preservation
- Examination and analysis of cloud based data or artefacts
- Utilize proprietary and open source tools for doing forensic analysis
- Ability of remote acquisition of data
- Ability to reconstruct events in the Cloud
- Ability to trace an event and assess the current state of an event in the Cloud
- Understanding of laws, SLA etc., in cases of multi-jurisdiction and multi-tenancy environment
- Ability to collect, analyse and correlate logs across multiple systems in cloud.
- Conducting forensic analysis combined with an ability to accurately record full documentation in support of the investigation
- Thorough understanding of standard evidence handling procedures
- Proficient with forensic techniques and the most commonly used computer forensic tools

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate / M. Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication
- Should have experience in performing security incident response and/or digital forensic analysis.

Desired certification/s

- Industry certifications like CompTIA Cloud Essentials, GCFA, CHFI or other relevant certification

6. Name of the profile: Crypto Analysts

Number of Position/s: 04

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	1-3 years	02	Rs.1,53,550
Level 2	More than 3 years	02	Rs. 2,31,300

Key responsibilities and required skill sets

- Examine artefacts related to cryptographic and various crypto storage applications or services.
- In-depth knowledge of investigations in encryption concepts, chain of dependencies etc.

- Perform analytics on crypto products like crypto-currencies using available tools as well as through developing bespoke tools
- Identifying any weakness in existing cryptography systems with a view to making them more secure.
- Identifying ways and means to work with encrypted data to aid LEAs.
- Conducting forensic analysis combined with an ability to accurately record full documentation in support of the investigation
- Thorough understanding of standard evidence handling procedures
- Proficient with forensic techniques and the most commonly used computer forensic tools
- Excellent oral and written communication skills
- Understands user and machine authentication and encryption mechanisms.
- Expertise in token technologies, PKI, OAuth and SAML
- Experience with security protocols including SSL/TLS, HTTPS, PGP, AES, DES, SSH, SCP, Kerberos, IPSEC
- Strong working and practical knowledge of TCP/IP and UDP/IP networking layer.
- Ability to write in-house tools, extenders and automated scripts
- Security expertise in one or more of: C, C++, x86, ARM etc.

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate / M. Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

- Industry certifications like CEH / OSCP or other equivalent certification

Annexure-III

1. **Name of the profile: Data Analysts**
   Number of position/s: 2

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	1-3 Years	01	Rs.1,55,500
Level 2	More than 3 years	01	Rs.2,33,250

Key responsibilities and required skill sets

- The ideal candidate must possess strong analytics skills and critical thinking skills
- Ability to work with large amounts of data, facts, figures, and analyse it to produce required insights
- In-depth knowledge and understanding of data structure , data mining and analytical tools
- Ability to work with law enforcement personnel, industry experts and other stakeholders for developing actionable information on cybercrime
- Ability to utilize available information to anticipate cyber-attacks, and make informed prediction for staying ahead of cyber threats
- Experience with scripting and development skills in Python/Pearl with deep comprehension of regular expressions
- Big Data experience with tools like MongoDB, SAS, Hadoop, Cloudera
- Knowledge of general networking and security knowledge in areas such as Firewalls, TCP/UDP, Routing/Switching, DNS, NAT, Packet Tracing and Analysis, etc.

Essential qualification/s

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering graduate/ M.Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

Industry Certifications in the area of Data Analysis like Cloudera Certified Administrator for apache Hadoop (CCAH), Cloudera certified Professional: Data Scientiest (CCP:DS), EMC data scientist associate (EMCDSA); Certified Analytics Professional (CAP), IBM Certified Data Architech/ Engineer MongoDB certified DBA associate, Post graduate Diploma/ Program in Big Data Analytics or any other equivalent certifications.

2. **Name of the profile: Malware researchers**
   Number of position/s: 1

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	1-3 Years	01	Rs.1,55,500

Key responsibilities and required skill sets

- Understanding of the Malware management process and tools, performing signature analysis
- Use expertise. in malware reverse engineering and analysis to evaluate and analyse complex malicious code through the use of tools, including disassemblers, debuggers,

hex editors, un-packers, virtual machines, and network sniffers

- Develop, configure and use sandbox for malware analysis
- Conduct static and dynamic analysis for known and suspected malware files
- Investigate instances of malware attacks and malicious codes to determine attack vector and payload, and to determine the extent of damage and data exfiltration
- Participate in research and development of malware protection tools & capabilities
- Perform behaviour analysis of malware codes/ Pattern analysis of malware codes/ manual unpacking of protected malicious executables/ subvert anti-analysis mechanism built into malware
- Prepare threat reports and malware attack trends
- Reconstruct infection artefacts
- Use of memory forensic tools
- Ability to identify and classify of malware families based on standard taxonomy
- Collect structured and unstructured data from enterprise file servers, email, database systems
- Utilizes understanding of attack signatures, tactics, techniques and procedures associated with advanced threats
- Analyse the attack/exploit capability of malware, document, and catalogue findings and Develop necessary procedures or scripts to identify such data in future
- Analyse collected media for defensive cyber operations and understand adversary technical capabilities and Tactics, Techniques and Procedures (TTP) methods of employment
- Understanding of tools and technologies to analyse zero day attacks
- Present tactical and strategic intelligence about threat actors, methodologies, and motivations based on malware research and develop methods of tracking and detecting malicious activity within a network
- Use various tools and techniques to analyse malicious document files, executables and web-based malware
- Prepares and presents briefings as subject matter expert as required. Alert security personnel's in the organization about the new malware threats and its behaviour
- Understanding of x86, ARM, and x64 architectures
- Understanding of network protocols and networking concepts
- Strong understanding of Windows Operating System Internals and Windows APIs
- In-depth knowledge and understanding Cybercrime prevention and mitigation
- Deep understanding of Software development and system design
- Hands on experience with a combination of the following languages: C/C++/C#/Python/Ruby
- Microsoft SQL Server, Hadoop, Reverse engineering, Web technologies
- Experience with Machine Learning

Essential qualifications

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering graduate/ M.Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

- Industry certifications like CEH / OSCP / GIAC (Global Information Assurance Certifications) Reverse Engineering Malware (GREM)/ Certified Expert Malware Analyst (CEMA) or any other similar certification

3. **Name of the Profile: Open Source Intelligence Professional**
Number of position/s: 4

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee (INR)
Level 1	3-5 Years	02	Rs. 1,55,500
Level 2	6-8 years	02	Rs. 2,33,250

Key responsibilities and required skill sets

- Monitor open source content including social media platforms and other web space to identify and report any cybercrime/ anti-national/ dangerous/ undesirable activities.
- Using data from social media, open sources, search engines, public records, and the deep web to compile detailed reports on cybercrime, criminals and criminal infrastructure
- Review unlawful and suspicious content in open source and escalate violations to the appropriate govt. department
- Responsible for co-ordinating with the social media platforms and other online platforms
- Collect, organize, analyse and develop reliable actionable intelligence about cybercrime, criminals, criminal infrastructure from open sources
- Information Security certification are a strong plus
- Must have advanced understanding of how to use open-source including social media for intelligence.
- Must have strong communication skills (verbal, written)
- Proven ability to work both independently and as a team and present/develop ideas
- Ability to work effectively with technical and non-technical business owners.
- Ability to communicate (verbal and written) with stakeholders in non-technical terms.
- Experience with multiple social media platforms.

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate/ M.Tech; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

- Industry certifications related to OSINT/ social media analytics/ Cyber Defence/ information Assurance/ Experience of working with open source social media based investigations

4. **Name of the profile: Programme Manager**
Number of position/s: 1

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee range (INR)
Level 2	More than 3 years	01	1,39,950

Key responsibilities and required skill sets

- Formulate, organize and monitor inter-connected theme based projects
- Decide on suitable strategies and objectives
- Coordinate cross-project activities

- Develop and control deadlines, budgets and activities
- Apply change, risk and resource management
- Assume responsibility for the program's people and stakeholders
- Resolve projects' higher scope issues
- Prepare reports for program directors
- Excellent Knowledge of performance evaluation and change management principles
- Ability to work closely with stakeholders from diverse background
- Outstanding leadership and organizational skills
- Excellent communication skills
- Excellent problem-solving ability
- Excellent project management skills

Essential qualification

- Bachelor in IT/ Computer Science/ Electronics and Telecommunication; or
- Engineering Graduate IM.Tech ; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

- Industry certifications like ITIL / PMP / Prince2 or other equivalent certification

5. Name of the profile: Subject Matter Expert (SME) for Cybercrime Investigations
Number of position/s: 1

Description	Relevant years of experience	Number of position/s	Indicative monthly professional fee range (INR)
Level 2	More than 3 years	01	Rs.1,71,050

Key responsibilities and required skill sets

- In depth experience with industry standard digital forensic methodologies, including evidence handling, chain of custody procedures, and commonly used Forensic
- Ability to clearly document and communicate findings, opinions, and recommendations to both technical and non-technical audiences.
- Collect, process, and analyse electronically stored information (ESI) obtained from network, cloud and end user digital sources in accordance with industry standards Excellent knowledge of digital hardware, experience in different file systems & operating systems artefacts
- Ability to work under limited supervision, work with different investigation teams to aid in investigation and to plan and execute forensic support for both simple and complex investigations
- Knowledge of computer science and laws related to computer evidence recovery as well as procedures for the collection, preservation and presentation of computer evidence
- Examine and perform comprehensive technical analysis of computer-related evidence and information stored on a device(s) during the course of an investigation
- Provide recommendations for identification, collection and preservation of digital evidence.
- Knowledge of computer forensic investigation and electronic discovery
- Knowledge of methods to recover data which has been deleted/erased, fragmented, hidden, or encrypted from data storage devices

Essential qualification

- Bachelor in IT/ Computer Science/ E!ectronics and Telecommunication; or
- Engineering Graduate/ M.Tech; or
- BCA / MCA or any other post graduate degree in the area of IT/ Computer Science/ Electronics and Telecommunication

Desired certification/s

- Industry certifications like CEH, CHFI, OSCP, GCFA, GCIH, GIAC, ENCE CFE, or equivalent certification related to forensics domain