For Website

Engagement of Consultants in NTRO

1. Overall Requirement

Following requirements have to be filled purely on contract basis for at least **one year**, for posting at New Delhi.

SN	Domains	Requirement			Total
		Consultant Level-3	Consultant Level-2	Consultant Level-1	
a)	Android Security Researcher	1	1	-	**2**
b)	iOS Security Researcher	1	1	-	**2**
c)	Windows Security Researcher	4	2	-	**6**
d)	Linux Security Researcher	1	1	-	**2**
e)	Network Security Researcher	-	1	1	**2**
f)	Malware Researcher	2	3	1	**6**
	Total	**9**	**9**	**2**	**20**

2. Age, Experience and Essential Qualification criteria

SN	Positions	Age		Minimum Experience	Essential Qualification
		Min.	Max.		
a)	Consultant Level-3 (CODE: L3)	22	35	Between 3 to 5 years in specific Cyber domain from recognized Govt. / Private Organization	First Class M.E. / M. Tech / M.S. in Computer Science / Information Technology / Cyber Security / Information Security or equivalent
b)	Consultant Level-2 (CODE: L2)	21	31	Between 1 to 3 years in specific Cyber domain from recognized Govt. / Private Organization	First Class BE / B. Tech in Computer Science / Information Technology / Cyber Security / Information Security or equivalent;
c)	Consultant Level-1 (CODE: L1)	21	25	Between 0 to 1 year from recognized Govt. / Private Organization	First Class BE / B. Tech in Computer Science / Information Technology / Cyber Security / Information Security or equivalent

3. Domain-wise Requirements (Total Requirement: 20)

3.1. Android Security Researcher (Total Requirement: 2, CODE:AN)

Position	Min-Max Age	Minimum Experience	No. of Requirement
Consultant Level-3	22-35	3-5 years	1
Consultant Level-2	21-31	1-3 years	1

a) Key responsibilities

- Analyzing the design of Android-based malwares
- Vulnerability analysis of Android System
- Research on Android exploits

b) Desired skillsets

- Understanding the design of android-based applications
- Knowledge in security features of Android System
- Programming skills in JAVA / Kotlin / C / C++ / C# / BASIC / Corona / Cordova / Lua / PhoneGap / Python / Ruby / Java script or relevant
- Hands-on experience of tools used for Android Penetration Testing / Reverse Engineering of malware

c) Desired Certification

- CND / CEH / ECSA / LPT / OSCP / GASF / ICMDE

3.2. iOS Security Researcher (Total Requirement: 2, CODE:IO)

Position	Min-Max Age	Minimum Experience	No. of Requirement
Consultant Level-3	22-35	3-5 years	1
Consultant Level-2	21-31	1-3 years	1

a) Key responsibilities

- Analyzing the design of iOS-based malwares
- Vulnerability analysis of iOS System
- Research on iOS exploits

b) Desired skillsets

- Understanding the design of iOS-based applications

- Knowledge in security features of iOS System
- Programming skills in C / C++ / C# / Objective-C / Swift / iOS SDK / React-Native / JAVA / Perl / Python / Ruby or relevant
- Hands-on experience of tools used for iOS Penetration Testing / Reverse Engineering of malware

c) Desired Certification

- CND / CEH / ECSA / LPT / OSCP / GASF / ICMDE

3.3. Windows Security Researcher (Total Requirement: 6, CODE:WI)

Position	Min-Max Age	Minimum Experience	No. of Requirement
Consultant Level-3	22-35	3-5 years	4
Consultant Level-2	21-31	1-3 years	2

a) Key responsibilities

- Analyzing the design of Microsoft Windows-based malwares
- Vulnerability analysis of Microsoft Windows System
- Research on Microsoft Windows exploits

b) Desired skillsets

- Understanding the design of Microsoft Windows-based applications, Windows Internals, Windows API, Powershell
- Knowledge in security features of Microsoft Windows System
- Programming skills in C / C++ / C# / Shell coding / JAVA / PHP / Lua / Perl / Python / Ruby / Java Script or relevant
- Hands-on experience of tools used for Microsoft Windows Penetration Testing / Reverse Engineering of malware

c) Desired Certification

- CND / CEH / ECSA / LPT / OSCP

3.4. Linux Security Researcher (Total Requirement: 2, CODE:LI)

Position	Min-Max Age	Minimum Experience	No. of Requirement
Consultant Level-3	22-35	3-5 years	1

Position	Min-Max Age	Minimum Experience	No. of Requirement
Consultant Level-2	21-31	1-3 years	1

a) Key responsibilities

- Analyzing the design of Linux-based malwares
- Vulnerability analysis of Linux System
- Research on Linux exploits

b) Desired skillsets

- Understanding the Linux Internals and design of Linux-based applications
- Knowledge in security features of Linux System
- Programming skills in C / C++ / Shell coding / JAVA / PHP / Lua / Perl / Python / Ruby / Java Script or relevant
- Hands-on experience of tools used for Linux Penetration Testing / Reverse Engineering of malware

c) Desired Certification

- CND / CEH / ECSA / LPT / OSCP

3.5. Network Security Researcher (Total Vacancy: 2, CODE:NE)

Position	Min-Max Age	Minimum Experience	No. of Requirement
Consultant Level-2	21-31	1-3 years	1
Consultant Level-1	21-25	0-1 year	1

a) Key responsibilities

- Analyzing the design of malwares used for exploiting IT-Network
- Vulnerability analysis of IT-Network
- Research on tactics, techniques and procedures used by Malwares to exploit an IT-Network

b) Desired skillsets

- Understanding the networking concepts, networking protocols, design of network-based applications, working of networking devices and technologies like routers, UTM, DNS infrastructures etc.

- Knowledge in various security features applied over an IT-Network
- Knowledge in functioning of Web technologies / Database management System / Cloud Technologies or relevant
- Programming skills in C / C++ / Shell coding / JAVA / PHP / Lua / Perl / Python / Ruby / Java Script or relevant
- Hands-on experience of tools used for Network Discovery / Penetration Testing / Reverse Engineering of Malware

c) Desired Certification

- CND / CEH / ECSA / LPT / OSCP / GREM / CEMA) / CCNA / CCNP

3.6. Malware Researcher (Total Vacancy: 6, CODE:MA)

Position	Min-Max Age	Minimum Experience	No. of Requirement
Consultant Level-3	22-35	3-5 years	2
Consultant Level-2	21-31	1-3 years	3
Consultant Level-1	21-25	0-1 year	1

a) Key responsibilities

- Analyzing the design of complex malicious code used in Malwares
- Management of Malwares / Sandbox environments
- Reverse Engineering of Malwares
- Research on Malware exploits

b) Desired skillsets

- Understanding of the Malware Lifecycle and Malware management process
- Understanding of attack signatures, tactics, techniques and procedures used by Malwares
- Reverse engineering and analysis of Malwares
- Understanding of assembly languages used in x86, ARM, x64 architectures
- Programming skills in C / C++ / C# / Shell coding / JAVA / PHP / Lua / Perl / Python / Ruby / Java Script or relevant

- Hands-on experience in disassembler tools, debugger tools, hex editor tools, un-packer tools or relevant

c) Desired Certification

- CND / CEH / ECSA / LPT / OSCP / GREM / CEMA / CHFI

4. Certification Weightage

Total 13 (thirteen) certifications have been considered for assessment of the candidates. These certifications have been categorized into three levels named “Basic”, “Intermediate” and “Advanced” depending on the difficulty levels as defined by the Certification Provider.

Additional weightage will be given to the candidates based on the level of certification held by them.

A. Basic Level (Weightage value: 8)

(a) CCNA: Cisco Certified Network Administrator
(b) CEH: Certified Ethical Hacker
(c) CND: Certified Network Defender

B. Intermediate Level (Weightage value: 12)

(a) CCNP: Cisco Certified Network Professional
(b) CHFI: Computer Hacking Forensic Investigator
(c) ECSA: EC-Council Certified Security Analyst
(d) ICMDE: IACIS Certified Mobile Device Examiner

C. Advanced Level (Weightage value: 20)

(a) CCIE: Cisco Certified Inter-Networking Expert
(b) CEMA: Certified Expert Malware Analyst
(c) CCNP: Cisco Certified Network Professional
(d) GASF: GIAC Advanced Smartphone Forensics
(e) GREM: GIAC Reverse Engineering Malware
(f) LPT: Licensed Penetration Tester

Any other relevant recognized certification may be considered and included by the Review Board depending on proficiency and competency of the Certification.

6. Vacancy CODE

6.1. Candidates have to mention a “Vacancy CODE” against the vacancy they are interested in. The “Vacancy CODE” comprises of the “Position CODE” appended by the “Domain CODE”. List of “Position CODE” and “Domain CODE” is given below:

Position CODE

SN	Positions	CODE
a)	Consultant Level-1	L1
b)	Consultant Level-2	L2
c)	Consultant Level-3	L3

Domain CODE

SN	Domains	CODE
a)	Android Security Researcher	AN
b)	iOS Security Researcher	IO
c)	Windows Security Researcher	WI
d)	Linux Security Researcher	LI
e)	Network Security Researcher	NE
f)	Malware Researcher	MA

For example, a candidate interested for the position “Consultant Level-1” in domain “Windows Security Researcher” has to use Vacancy CODE “L1WI”.

7. Recruitment and Selection Process

7.1. How to Apply

7.1.1. The application performa **Annexure ‘A’** shall be available as separate downloadable file to the applicants on NTRO official website “https://ntro.gov.in” along with this advertisement.

7.1.2. Interested eligible candidates have to download the performa **Annexure ‘A’** from the website and fill it in the soft copy mode. The application has to be filled up and forwarded as per instructions given in the “**Information”** tab of the application performa.

7.1.3. Application generated result in **JSON** form shall be sent to official mail-id **recruitment.apply@gov.in** from the applicant's valid e-mail id latest by **14 March 2020 (Note: No additional attachment shall be sent to the email-id).**

7.1.4. Hard copy of the duly filled application performa alongwith two passport photographs and other relevant enclosures shall be sent by post, so as to reach the following address by **20 March 2020**.

Deputy Director (Estt)
National Technical Research Organisation (NTRO)
Block-III, Old JNU Campus
New De;lhi 110067

7.1.5. Candidates are requested to send the application in **soft copy** to official email id as well as **hard copy** to official postal address on scheduled dates, failing which their candidature will be treated as invalid.

7.1.6. Each applicant shall be permitted to send a single copy of application performa. Candidates interested for multiple positions, may fill the details in the single application performa against the relevant column.

8. Selection Process (PHASE-I: Screening)

8.1. Screening of the application has to be carried out based on following criteria:

8.1.1. Adequacy in adopting the given rules in filling and sending application performa to the employer.

8.1.2. Age criteria as per position applied

8.1.3. Educational qualification criteria as per position applied

8.1.4. Experience criteria as per position applied (Note: For Consultant level 2 and 3 along with the required years of experience, "relevant work experience" with respect to the cyber domains applied must be strictly matched).

8.2. Eligible candidates meeting all above criteria may be shortlisted for the next phase of selection process.

8.3. Shortlisted candidates shall be intimated regarding their selection for next phase of selection process along with the date of Interview through their email ID. **Candidates are requested to check their email ID and our website "https://ntro.gov.in" for regular updates.**

9. Selection Process (PHASE-II: Interview)

9.1. The shortlisted candidates shall appear for the interview on the intimated schedule date with hardcopy of their application performa and original copy of enclosures.

9.2. Candidates shall be required to fill-up and sign an “Expected Emolument Certificate” (performa as defined in Appendix ‘E’), stating his / her expected monthly gross emolument for the interested vacancy.

9.3. Evaluation process for the Interview is given below:

9.3.1. Candidates shall be evaluated in the Interview purely based on their performance along with relevant certification and work experience.

9.3.2. Overall score of the candidates shall depend on three different factors like “Certification”, “Experience” and “Performance in the Interview”.