Booz | Allen | Hamilton

GLOBAL NETWORK ANALYSIS Profiles (Ft Meade MD)

Digital Network Intelligence Analysis provides network intelligence analysis support within multiple SIGINT development offices to high-profile government clients for a rapidly growing team. Provide a wide range of network intelligence analysis, including basic research, protocol analysis, and logical and physical mapping of data focusing primarily on the network through the application layers of the OSI model, and report the results of the analysis. Perform communications and user discovery using various tools, techniques, and processes, including social engineering and passive information gathering to enable research and analysis of complex digital communications and application layer protocols.

SIGINT Network Analysis supports with a specific focus analyzing complex data and telecommunications target networks of interest. Provide a wide range of network analysis, including basic research, protocol analysis, and network topology mapping of traffic through different layers of the OSI model and report the results of analysis. This support involves baselining the client's knowledge of the current implementation of these technologies in target areas of interest. In addition, the analyst will be required to devise SIGINT analytical and collection strategies to pursue access and exploitation against these modes of target communications.

Malware Analysis evaluates and analyzes complex malicious code through the utilization of tools such as disassemblers, debuggers, hex editors, un-packers, virtual machines, and network sniffers. Provide the findings in a technical report with details of the malware, identification parameters, advanced capabilities and mitigation strategies. Performance of research in the area of malicious software, vulnerabilities, and exploitation tactics will also be necessary. The ideal Malware Analyst must be well versed in multiple disciplines: network analysis/forensics, forensics/OS heuristics, reverse engineering.

SIGINT Research & Target Development (SRTD) provides support with a focus on SIGINT analysis techniques which may include but are not limited to contact chaining, digital network intelligence analysis, target technology and systems analysis, military analysis, and social network analysis. The analyst is responsible to devise and contribute to SIGINT analytic and collection strategies to pursue pertinent modes of communication and/or technologies. Extensive reach-back capabilities of military operations, intelligence community resources, and/or intelligence technologies in such areas as telecommunications, collection, signals analysis, imagery analysis, computer science, electronic warfare and/or nuclear/biological/chemical warfare.

Successful Candidate Attributes:

- Strong background in government consulting (Knowledge of NSA client office organizations is preferred) and/or former military experience
- Superior analytical skills - ability to generate insight and solve complex client problems using proven analytical methodologies/techniques
- Strong oral and written communication and presentation skills
- Strong ability to lead executive and senior leadership teams through workshops, strategic discussions and recommendations
- 4+ years of demonstrated project/ program management experience managing to plan and budget, staffing/ utilization requirements, and client management
- Demonstrated experience leading and working on complex proposals for public/private sector clients, developing new client business and providing thought leadership on client organizations with an eye towards business development opportunities.
- Worked in complex, matrix environments leveraging resources and capabilities to provide the best possible results to client organizations
- Passion for developing and mentoring staff (high performing team orientation)
- Self-driven towards accomplishing mission based initiatives; not averse to risk taking

Must Haves:

- TS/SCI clearance with polygraph
- Undergraduate/advanced degrees in a related field or applicable industry-recognized certifications (Net+, Security+, CEH, and/or CCNA) are desirable
- Applicable work experience (minimum of 2 years) - knowledge of the protocols within the TCP/IP suit and the many software services that use them; e.g. consulting, military intelligence, project management
- Profound knowledge of the Microsoft Windows Internals (file system, registry, administrative settings…etc)
- Ability to multi-task/manage time (involvement in multiple projects and internal/external activities/organizations)
- Sustainability and repetition of success (i.e. job hoppers typically do not have run time to make impact long-term)

Booz | Allen | Hamilton

Key Business and Team Factors:

- Rapidly growing, global technical expertise in Malware Analysis, Digital Network Intelligence Analysis and SIGINT Network Analysis that intersects across all markets and sectors on both the defensive and offensive lines
- Fluid set of service offerings aimed at senior level parts of the organization
- Opportunity to build a business while continuously improving upon deep consulting skills (analytics, strategic and critical thinking senior voice)
- Extremely interesting work: a) expanding & utilizing critical thinking skills, b) learning new things, c) variety of topics & deliverables
- Ability to make a difference in multiple and varied organizations
- High level of responsibility and autonomy
- Intensive and comprehensive training for long term professional development
- Manage and work directly with intelligent, motivated individuals
- Competency based performance system that articulates a career development roadmap for seniors
- Structured and informal mentorship and executive coaching programs
- Governance roles and responsibilities as you become more senior

Key Credentials We Look For:

- Nessus
- Network configuration
- DSL
- Cable modem
- Fiber optic technologies
- Reconstruct network, testing
- TCP/IP
- ATM
- Routing
- Switching
- Router
- Telecommunication- all source
- Ethernet
- Frame relay
- LAN
- Computer network
- OSI model
- Digital network
- Network analysis
- Network topology
- Mapping of traffic
- Exploitation
- Exploit
- Vulnerabilities
- Wireshark
- Ethereal
- Topdump
- Pcap
- NMap
- Packet analysis
- SMIP
- DNS
- Ethical Hacker
- CEH
- CCNA
- Red team
- DNS
- Registry Info (whois)
- Traceroute

Booz | Allen | Hamilton

- ESRI
- ArcView
- ArcGIS
- ArcMap
- ArcCatalog
- ArcExplorer
- ArcInfo
- ArcObjects
- Erdas Imagine
- Google Earth
- Satellite Tool Kit (STK)
- Remote sensoring
- Data mining
- Open source research
- Sniffer
- Programming Languages (i.e. VB, .net, C++, Python, Avenue, Java, perl, Geodatabase Oracle
- Wireless
- 802.11
- SNIP

Professional Development Programs:

- MECCAP
- JOCCAP
- PGIP
- UGIP
- NETA 3001
- NETA 2008
- BDNA
- iDNA
- aDNA

SIGINT:

- ANCHORY
- ASSOCIATION
- DISFIRE
- MAINWAY
- BANYAN
- CULTWEAVE
- NUCLEON
- PATHFINDER
- PLUS
- Technical Report
- Collection Management
- Normalization
- CPE
- HIGHTIDE
- SKYWRITER
- AMHS
- Reporting
- Report
- Reporter
- Serialized
- Product
- Editing
- Edit
- Editor
- PINWALE
- Network Intelligence

Booz | Allen | Hamilton

- GLOBAL BROKER
- SIGINT NAVIGATOR
- OCTSKYWARD
- CNE PORTAL
- SURREY/CADENCE/OCTAVE
- BLACKPEARL
- XKEYSCORE
- TRAFFICTHIEF
- TAROTCARD
- TUNINGFORK
- TAO
- PUZZLECUBE
- SIGINT
- Target Development
- Geographic Information Systems (GIS)
- Geospatial Metadata Analysis (GMA)
- Geo Boot Camp
- Spatial Analysis/ Thinking
- Temporal Analysis
- MARINA
- Target Communication

Defensive:

- Reverse Engineering
- Malware
- Malware Analysis
- IDA Pro
- OllyDbg
- Computer Emergency Response
- Team (CERT)
- Assembly Language Programming
- Rootkit
- Virus
- Worm
- Botnet
- Incident Response
- WinDbg
- Rootkit
- Firewall
- Network Defense
- Intrusion Detection
- SNORT
- DRAGON
- Signature
- Signature Development
- Portable Executable
- Reverse Engineering
- PERL
- PYTHON
- Script
- Intrusion
- Intrusion Analysis
- IDS
- Mitigation Strategies
- Mitigation
- Hacker
- Hacking
- Hacker Techniques

Booz | Allen | Hamilton

- Network Enumeration
- Network Scanning
- Network Probing
- Exploitation
- Malicious Code
- Pen Testing
- Penetration Testing
- Sensor
- Network Forensics
- Media Forensics
- Forensics
- SQL Injection
- Buffer Overflow
- Denial Of Service
- DoS
- Wireshark
- Vulnerability Analysis
- Vulnerability Assessment
- Red Team

Clearance:
Applicants selected will be subject to a security investigation and may need to meet eligibility requirements for access to classified information; TS/SCI clearance with polygraph is required.
We are proud of our diverse environment, EOE, M/F/D/V.

Booz | Allen | Hamilton, as you may know, is undeniably one of the fastest growing (and one of the most profitable companies) to remain private, currently ranked 4th of the top 50 firms. My role here is to identify ideal external professional profiles that compliment the BAH business model and culture. With talent being our primary commodity, we pride ourselves on seeking out individuals with impressive and solid backgrounds and offering them opportunities to develop skills beyond their current expertise.

For more information, please contact DAPHNE MAHOTIERE at Booz Allen Hamilton (mahotiere_daphne@ne.bah.com) Thank you!