Intelligent Security Operations Consultant

DXC Technology (NYSE: DXC) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner alliance combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.

Travel: Up To 75% if needed. Generally between 25%-50%.

Our WW Security Consulting Group is looking for a Senior level Digital Forensics and Incident Response Consultant to lead our consulting engagements with our various clients. **The ideal candidate will be a good client communicator and team leader with in depth knowledge and understanding of APT actors and threats and how to deal with APT incidents as part of a wider incident response (e.g. security enhancement etc.)**. A complete knowledge of live security incident management and handling including leading, teaming, analysis and remediation (min 5 years' experience in commercial or government environments). Comprehensive understanding of security improvement planning, and an ability to make in depth recommendations regarding same. Flexible and dynamic working approach and willing to work 24/7 in delivery capability, often travelling away from home at short notice for extended periods.

The services offered will fall into four main fields:

• Digital investigations incorporating Computer and Network Forensic investigations
• E-Disclosure
• Computer Security Incident Response
• Data Recovery, Deletion and Destruction

Description of Business

The offering is delivered in order to fulfill the needs of the customer and DXC as follows:

• The ability to carry out sensitive e-Discovery and Computer Forensic inquiries
• The ability to provide a highly skilled Computer Security Incident Response team that is able to react on a 24/7 basis
• The ability to effectively identify, recover and analyze seats of relevant information and evidence
• To be able to present this information in an appropriate manner
Although the services may use core resources that are similar, the skill sets and requirements for each can be diverse. Therefore nature and type of individuals required to deliver the services can vary significantly depending upon what is being delivered.

Education:

• BSc or higher in a Computer Forensics; OR BSc in a relevant digital investigation/security subject; OR BSc qualification and relevant IR/Forensic post degree qualifications; and Post degree qualification in IR/Forensics (e.g. SANS)
• MSc degree in a field with emphasis on computer security and investigations, preferred
• Demonstration of a continuing ability to self-teach
• CISSP, GCIH, GIAC, GCFE, GREM SANS Certifications, EnCE, ACE (at least two of these)

Experience and Skills:

• 10 + Years' Experience in IT Security and Investigations
• Demonstrated experience of leading teams of investigators on diverse and complex investigations
• Demonstrated capability in handing large scale investigations involving Targeted Threat Actors
• Must have a deep and current understanding of the tools techniques and tactics of Targeted Threat Actors and remain up to date with current and future trends
• Mentor and or identify training to personnel
• Ability and willingness to be involved with APT security research community to maintain knowledge and garner intelligence
• Demonstrated presentation skills, able to articulate and present to a wide audience from technical to the board room
• Demonstrated experience of maintaining and developing Digital Investigation Service capabilities
• Demonstrated experience of contributing to IT Security projects
• Demonstrated experience of SOC, Digital Forensic and Incident Response operations.
• In depth knowledge of current targeted threat intrusion scenarios and capable of reproducing them in a lab environment
• Targeted Threat Intrusions are a complex issue, requiring a logical, intelligence driven human response to counter it
• Good understanding of the implications of Data Privacy legislation
• Good understanding of forensic and incident response methodology and tooling
• Good understanding of IT Security to protect and monitor the enterprise
• Possesses as a unique blend of experience, vision, technical, and interpersonal skills that are required for such a position
• Excellent team and case management skills
• Excellent reporting (written and verbal) skills – Client (to C Level) and internal

Workload

• 80% of time will be spent in the field investigating Targeted Threat Intrusions (billable to client), collaborating with senior staff, and mentoring junior staff on current cases. Willing to travel
• 20% Research and administration

Please note the above statements describe the general nature and level of work only. They are not a complete list of all required responsibilities, duties and skills. Other duties may be added, or this description amended at any time.

DXC Technology is an equal opportunity employer. We welcome the many dimensions of diversity.

Accommodation of special needs for qualified candidates may be considered within the framework of the DXC Accommodation Policy.

DXC benefits package includes state of the art medical, dental, vision, flex spending, 401K, life insurance, PTO, paid holidays and additional sick days, etc.