Arete
Incident Response

Role Description

JOB TITLE: Digital Forensic Analyst
REPORTS TO: Director of the Tiger Team

SUMMARY

The Forensic Analyst role supports the Forensic Lead and Senior Analyst on active projects assigned to them on the respective Tiger Team. The Forensic Analysis performs triage level analysis independently on data collections (e.g. Skadi, SentinelOne, Logs, etc.) and more deep dive advanced analysis under the direction and guidance of a Senior Analyst or Forensic Lead. The Forensic Analyst will contribute findings for the final report under the direction of the Forensic Lead or Senior Analyst.

ROLES AND RESPONSIBILITIES

- Providing daily updates to Senior Forensic Analysts and Forensic Lead.
- Escalating questions and issues to your Forensic Lead.
- The analyst will help keep track of project hours and will map their hours in the Master Planner so the Forensic Lead can allocate projects effectively.
- Investigate breaches leveraging forensics tools including Encase, FTK, X-Ways, SIFT, Splunk, and custom investigation tools to determine source of compromises and malicious activity that occurred in client environments. The candidate should be able to perform forensic analysis on:
- Host-based such as Windows, Linux and Mac OS X.
- Firewall, web, database, and other log sources to identify evidence and artifacts of malicious and compromised activity.
- Cloud-based platforms such as Office 365, Google, Azure, AWS, etc.
- Perform analysis on identified malicious artifacts.
- Contribute to the curation of threat intelligence related to breach investigations.
- Excellent verbal and written communication and experience presenting technical findings to a wide audience of varying technical expertise.
- Be responsible for integrity in analysis, quality in client deliverables, as well as gathering caseload intelligence.
- Responsible for developing the forensic report for breach investigations related to ransomware, data theft, and other misconduct investigations.
- Must also be able to manage multiple projects on a daily basis.
- Help keep track of project hours and will map their hours in the Master Planner so the Forensic Lead can allocate projects effectively.
- Ability to work greater than 40 hours per week as needed.
- Other duties as assigned.

DISCLAIMER

The above statements are intended to describe the general nature and level of work being performed. They are not intended to be an exhaustive list of all responsibilities, duties and skills required personnel so classified.

SKILLS AND KNOWLEDGE

1. Must have at least 2+ years of incident response or digital forensics experience with a passion for cyber security (consulting experience preferred).

2. Proficient with host-based forensics, network forensics, malware analysis and data breach response.
3. Experienced with EnCase, Axiom, X-Ways, FTK, SIFT, ELK, Redline, Volatility, and open source forensic tools.
4. Experience with a common scripting or programming language, including Perl, Python, Bash, or PowerShell.

JOB REQUIRMENTS

- Experience in a security professional services consulting firm.
- One or more Digital Forensic and Incident Response Certifications such as GCFE, GCFA, GNFA, GCTI, GREM, CHFI, CCE, CFC, EnCE, and CFCE.
- BA/BS or MS degree in an IT– or Cyber–related field.

TERMS OF EMPLOYMENT

Salary and benefits shall be paid consistent with Arete salary and benefit policy.

DECLARATION

The Arete Incident Response Human Resources Department retains the sole right and discretion to make changes to this job description. Any employee making changes unauthorized by the Human Resources Department will be subject to disciplinary action up to and including termination.

EQUAL EMPLOYMENT OPPORTUNITY

We're proud to be an equal opportunity employer- and celebrate our employees' differences, regardless of race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability, or Veteran status. Different makes us better.