CYSIV

Job ID: 2018-0008

Sr. Incident Response Analyst

Job Summary

At Cysiv, we are building the future of cyber risk management as a service. Going above and beyond a traditional MSSP, we provide an advanced co-managed platform for detecting and responding to threats backed by enrichment, intelligence and data science. We are looking for a talented senior incident response analyst to help combat cybersecurity threats at all levels. The ideal candidate is interested in investigating computer crimes and breaches that make the headlines. Must be able to think like an attacker to stay one step ahead of them, or understand the operational security controls needed to detect, remediate, and prevent compromises. With strong technical skills and an eagerness to lead projects and work with our clients, the ideal candidate will also need to apply their forensics, log analysis, and malware triage skills to solve complex intrusion cases at organizations around the world. And they must be comfortable working in teams to tackle challenging projects, communicating with clients, and mentoring junior analysts.

Principle Duties and Responsibilities:

- L3+ Incident Response across multiple very large enterprise environments
- In-depth log analysis and investigation utilizing data from multiple security tools, infrastructure logs, application logs, and SIEM
- Proactive threat hunting and threat intelligence
- Mentor junior analysts: mentoring and teaching while on the job is a critical element to this role
- Work with the data science team to design, build, and validate custom indicators and detections across all data sources
- Utilize Cysiv technology to conduct large-scale investigations and examine endpoint and network-based sources of evidence.
- Recognize and codify attacker tools, tactics, and procedures in indicators of compromise (IOCs) that can be applied to current and future investigations.
- Develop comprehensive and accurate reports and presentations for both technical and executive audiences.
- Effectively communicate investigative findings and strategy to key stakeholders
- Work with security and IT operations at clients to implement remediation plans in response to incidents.

Requirements:

- Passion for log analysis: understanding what it means to log, digging into raw logs, indicators, alerts, and knowing how to put all the pieces together
- 5+ years of very large enterprise or Fortune 500 incident response
- Technical expertise in the following areas:
    - Network security monitoring, network traffic analysis, and log analysis
    - Static and dynamic malware analysis
    - Knowledge of Python and Bash scripting and willingness to learn
    - Very strong knowledge of Windows networking as told through security logs (AD, DHCP, Domain Controllers, File Shares, Windows Event Logs, etc.)
    - Very strong knowledge of security tools and their associated logs, such as proxies, firewalls, IPS/IDS, DLP, AV, Endpoint, Application, etc.
    - Very strong knowledge of email logs such as Exchange tracking logs, O365, Email AV, and other email-related security tools/logs
    - Very strong knowledge of at least one SIEM environment, such as Splunk, ELK, Arcsight, QRadar, etc.

- Case management systems
- Kill chain, Mitre ATT&K, and other models/frameworks

Additional Qualifications:

- Ability to successfully interface with both internal and external clients
- Ability to document and explain technical details in a concise, understandable manner
- Ability to manage and balance own time among multiple tasks, and lead junior staff when required

Location: Dallas

Cysiv provides equal employment opportunity for all applicants and employees. Cysiv does not unlawfully discriminate on the basis of race, color, religion, sex, pregnancy and childbirth or related medical conditions, national origin, ancestry, age, physical or mental disability, medical condition, family care leave status, veteran status, marital status, sexual orientation, or gender identity.