Ascension

Cyber Security Incident Response Specialist

Birmingham, AL

Summary
As an Associate with Ascension Technologies, you will have the opportunity to lead the design and execution of deployed business application systems. Mentors less-experienced staff with responsibility for their technical development.

Responsibilities:

- *Cyber Security Incident Response Team (CSIRT) Coordinator*: Will go through training for CSIRT Coordinator role and will be placed into on-call rotation schedule. Will be required to lead CSIRT events from detection to closure. Will be responsible for:
    - Leadership communications
    - Coordination of technical teams during the event
    - Completion of CSIRT checklists
    - Documentation of final analysis report
    - Completion of After Action Analysis and documentation
- *Advanced Threat Hunting*: Will be responsible for taking out of band Indicators of Compromise (IOCs) and completing threat hunts for identified IOCs within the Ascension environment. Requires use of multiple tools such as Tanium, Cylance, Chronicle, Fortinet, etc.
- *Advanced Triage of critical security events*: Will act as an escalation point for critical events. Will need to understand Ascensions infrastructure and workflows. Creating\enhancing process workflows, playbooks and processes to improve security response abilities
- Work with the team on developing new SEcurity Operations Center (SOC) capabilities and trends to improve incident response times and metrics. May require learning new technologies and how to integrate them into existing workflows and\or developing new workflows.
- Being able to work in a team environment:
- Able to work closely with others
- Share information

- Communication skills (verbal and writing)

Education:

- High school diploma/GED with 2 years of experience, or Associate's degree, or Bachelor's degree required

Work Experience:

- 1 year of experience required.
- 4 years of experience preferred.
- 2 years of leadership or management experience preferred.

Preferred Education:

- Bachelor's Degree
- Minimum of 5 years IT security experience
- CISSP certification or equivalent within a specialized security field
- Technical ability such as, scripting, security tools experience, log monitoring, malware analysis, memory analysis, etc
- Ability to multitask
- Understanding of basic network infrastructure components

More information / How to Apply:

https://jobs.ascension.org/jobs/5179179-cyber-security-incident-response-specialist