Senior Cybersecurity Engineer - SIEM
Auburn University

Job Title	Senior Cybersecurity Engineer - SIEM
Department	Chief Information Office
Institution	Auburn University Auburn, Alabama
Date Posted	Nov. 23, 2020
Application Deadline	Open until filled
Position Start Date	Available immediately
Job Categories	Professional Staff
Academic Field(s)	Information Technology
Apply Online Here	http://www.auemployment.com/postings/20359
Apply By Email	

Job Description

Job Summary
The Office of the Chief Information Security Officer is seeking applicants for the role of Sr. Cybersecurity Engineer (SIEM). Under general supervision, responsible for the planning, engineering, developing, implementing, and compliance monitoring of organization-wide information security programs. This role will be responsible for the maintenance and management of the Security Information and Event Management (SIEM) tools, such as Splunk and Azure Sentinel. This position is also responsible for assessing current logging and threat hunting gaps and developing dashboards and monitoring interfaces to fill those needs. Other cybersecurity duties may be assigned as needed.

Essential Functions
1. Assist in ensuring information security policies and procedures are followed.
2. Creates and maintains content (queries, dashboards, reports, alerts, etc.) in industry SIEM tools Splunk and Azure Sentinel.
3. Works in conjunction with the Security Operations Center (SOC) to assess gaps in monitoring and

Senior Cybersecurity Engineer - SIEM
Auburn University

develops content to rectify needs.
4. Manages the SIEM platform including log integration, app installation, SIEM upgrades, and platform maintenance.
5. Supports and participates in SOC engineering efforts such as tool and data integration, development of automation, scripts, testing of new tools and evaluation of new technologies.
6. Participates in risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and logging needs.
7. Assists in incident response efforts.
8. Communicates and coordinates with distributed information technology units and internal technical teams
9. Communicates and works with the Auburn University Audit, Compliance and Privacy department
10. May perform other related duties as assigned by the IT Manager.

Contact Information

Please reference Academickeys in your cover letter when applying for or inquiring about this job announcement.

Contact

,