Information Security Analyst

HEJ higheredjobs.com/search/details.cfm

LAMAR UNIVERSITY
MEMBER THE TEXAS STATE UNIVERSITY SYSTEM™

Information Security Analyst

Salary: $53,496.00 - $69,545.00 Annually
Location: Beaumont, TX
Job Type: Full-Time Staff
Job Number: 202600067
Closing Date:
Home Org: Information Technology
FLSA: Exempt

Job Summary

The Information Security Analyst (ISA) is a key entry level position in the Information Security team at Lamar University. The analyst reports to the Information Security Officer. He/she works with other technical teams on complex cross-functional projects and security initiatives. He/she is responsible for the day-to-day security of Lamar University information systems. This position is responsible for securing contemporary tools such as custom generative AI engines and preventing data loss.
The Security Analyst (AI & SecOps) monitors, detects, and responds to threats across our environment while operationalizing AI agents to enhance prevention, detection, and response. The role combines classic SOC analysis (log and alert triage, incident handling, vulnerability management) with AI-aware security: safeguarding AI services, models, and data pipelines; implementing guardrails for generative AI; and using AI/ML to accelerate investigations and reduce mean time-to-detect/respond.
This position sits in Security Operations within our security organization, with close collaboration across Governance/Risk/Compliance and Cloud/SIEM/SOAR teams.
This position does not qualify visa sponsorship.

Special Note: We are unable to provide visa sponsorship for this position. Candidates must be authorized to work in the United States without the need for sponsorship now or in the future.

Essential Job Functions

- Contribute towards development and management of the university's information security policies, procedures and technology standards.
- Participate in audit response activities.
- Coordinate with legal and compliance teams.
- The ISA will be responsible for vulnerability management program for the university. This includes conducting periodic scans, reporting and overseeing the remediation efforts for applications and services across the campus. Evaluate applied security controls in networks and applications (on-prem and cloud).
- Working with the ISO, the ISA will be responsible for coordinating penetration tests, reporting and associated remedial actions for applications and services across campus.
- The ISA will be responsible for establishing security standards for enterprise mobility management technologies.
- The ISA will be responsible assisting in the management of the University's Certificate Authority and the management of SSL certificates across campus.
- The ISA will be responsible for working closely with the computer emergency response teams, various law enforcement agencies and assist in management of information security incidents.
- Implement technologies to secure cloud services or work with cloud administrators to help enforce technical controls.
- Manage endpoint protection technology policies such as antivirus, advanced persistent threats (APT).
- Deploy and manage log aggregation and management technologies such as Microsoft Sentinel.
- Additional responsibilities will include threat modeling, coordination and reporting of application security requirements, and application security risk assessments and remediation.
- Secure AI usage: implement guardrails for generative AI/Copilot use (data loss prevention, prompt/response controls, safe-use policies), aligned with our org's AI security and ethics direction.
- AI model & pipeline risk: assess and mitigate risks such as prompt injection, jailbreaking, sensitive data leakage, model exfiltration, adversarial inputs, and data poisoning; recommend controls across data ingestion, fine-tuning, and inference.
- AI monitoring: design detections and telemetry for AI agents (e.g., aberrant calls, excessive data access, anomalous outputs), integrate into SIEM/SOAR for unified response.
- Third-party & supply chain: review AI SaaS vendors for security posture (privacy, retention, tenant isolation, red-team results) and collaborate with GRC on contractual guardrails.
- Responsible AI & compliance: partner with GRC to align AI use with policy, privacy, accessibility, bias testing, and documentation standards.

- Enablement: provide AI security and privacy awareness sessions and quick-reference guides for secure AI use across staff and faculty.

Minimum and Desired Qualifications
Minimum Qualifications:

- Bachelors in Computer Science or equivalent.
- 3-4 years system administration or network administration experience. Alternatively, 1-2 years of experience in an Information security role.
- Knowledge of AI risks (prompt injection, data leakage, adversarial examples) and practical guardrails for enterprise AI tools.
- Strong familiarity with prompts in generative AI products like CoPilot, Gemini, Grok and ChatGPT.

Desired Qualifications:

- Higher Education experience is preferred.
- Log query languages like KQL, SPL.
- Strong familiarity with prompts in generative AI products like CoPilot, Gemini, Grok and ChatGPT.
- Familiarity with Python.
- Preferred CISSP or CCSP. Other IT Security related certification a plus (i.e. Security+, CCNP, CSIH, I2C AI Security Certification). Candidate must be willing to pursue additional security certifications post-employment as mandated by regulations.
- Understanding of local, state, and federal laws relating to information security standards including but not limited to TGC 2054, Texas Administrative Code (TAC) 202 as well as subsequent updates thereof.
- Strong analytical writing and incident documentation skills; ability to communicate clearly with technical and non-technical stakeholders.

Supplemental Information
Key Competencies:

- Monitor and triage alerts from SIEM, EDR, NDR, CASB, email security, and cloud telemetry; escalate according to severity and runbooks.
- Investigate incidents (phishing, malware, identity compromise, lateral movement, data loss) and coordinate response, containment, eradication, and recovery with Infra/Cloud teams.
- Threat hunting using behavioral analytics and intelligence (OSINT, vendor feeds); document hypotheses, findings, and lessons learned.
- Vulnerability & exposure management: assist with scanning, prioritization, and remediation tracking; verify fixes and compensating controls.
- Security automation: contribute playbooks in SOAR to reduce manual toil (auto-enrichment, auto-quarantine, ticketing).
- Reporting: maintain incident tickets, daily/weekly dashboards, and metrics for leadership; support audit evidence collection.
- Strong verbal and written communication skills, including proofreading and use of correct grammar.
- Proficient with Microsoft Office applications (i.e., Word, Excel, PowerPoint), including the use of advanced features (e.g., track changes, document formatting, spreadsheet formulas, and charts).
- Demonstrate flexibility while working in a changing business environment.

Physical Requirements:

While performing the duties of this job, the employee is regularly required to see (close vision); sit; stand; operate a computer and other office machinery such as a telephone, copy machine, and printer; speak; and hear (in person speech, telephone, or remote speech).

Job Conditions:

- The employee is occasionally required to move about inside the office to access file cabinets, and office machinery.
- The employee works 8-5. Monday-Friday indoors.

Security Sensitive Statement: This position is designated as a critical infrastructure role and is subject to Cyber Intelligence Review in accordance with Executive Order GA-48. Additionally, this position is classified as Security-Sensitive and is thereby subject to the provisions of Texas Education Code 51.215, which authorizes the employer to obtain and review criminal history record information.
Lamar University is An Equal Opportunity Employer

Lamar University is proud to provide employment preference to veteran applicants in accordance with Texas 805 Government Code, Section 657.003.

This position is security-sensitive and thereby subject to the provisions of the Texas Education Code 51.215, which authorizes the employer to obtain criminal history record information.

To apply, please visit https://www.schooljobs.com/careers/lamar/jobs/5230921/information-security-analyst

jeid-ac6c3a9d9d436f488146216fd64ed4a6