Lead Engineer, Data Loss Prevention
Job Description

JOB INFORMATION

Job Code:	166039
Job Title:	Lead Engineer, Data Loss Prevention
FLSA Status:	Exempt
Supervisory:	May oversee staff, students, volunteers, agencies and/or resource employees.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Ensures the security of the most confidential enterprise data. Leads and helps define the data loss prevention program initiatives supporting university data protection requirements. Collaborates with and mentors team members in data loss prevention processes and procedures, assisting in formulating best practices for data loss-specific incident response investigation. Defines, manages, improves and updates processes and procedural documentation.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
	X	Bachelor's degree	Cyber Security	

Additional Education

Check here if experience may substitute for some of the above education.

X	Combined experience/education as substitute for minimum education

Work Experience

Req	*Pref*	*Work Experience*	*Experience Level*	
X		5 years	with data loss prevention software platforms supporting information security programs at large organizations	
	X	7 years	in information security	
	X	5 years	in data loss prevention engineering roles	

Additional Work Experience

Check here if education may substitute for some of the above work experience.

	Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	*Pref*	*Functional Skills*
X		Experience with CASB solutions (e.g., CloudSOC).
X		Knowledge of firewall theory and configuration, intrusion detection and internet architecture.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Ability to express complex technical security control concepts effectively.
X		Advanced systems administration skills for Windows Server and desktop platforms, Apple, Linux and databases.
X		Knowledge of Active Directory, VMWare, Microsoft Office 365 and on-premises Exchange, Google Apps, third party collaboration tools (e.g., Slack) and database structures (e.g., Oracle, MySQL, MSSQL).
X		Proven understanding of cyber security frameworks (e.g., NIST 800-53, NIST CSF, ISO-27001).
	X	Experience with design and implementation roles for large scale data loss prevention solutions.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Serves as a data loss prevention subject matter expert, determining, refining and updating rules, thresholds, requirements and policies. Builds and implements best practices, tracking adherence to and refinement of applicable security policies/standards. Mentors team members in security operations, forensic analysis, and IT operations, helping define investigative processes. Leads coordination of service/support needs with vendors, application support teams, and internal stakeholders through effective partnership, collaboration and communication. Applies information security principals to recommend, implement, support and improve data loss prevention/security controls.				
Ensures thorough testing of all data loss prevention solutions for functionality, efficacy and compatibility. Creates, tunes, and manages systems use cases, rules, configurations, permissions, processes, and procedures (e.g., operational runbooks and playbooks). Responsible for the ongoing maintenance and configuration of data loss prevention solution components, use cases, thresholds, rules and platform updates.				
Continuously monitors and develops data loss prevention metrics and assists with related system capacity forecasting. Supports incident response team with data loss incidents, analyzing, responding to and coordinating all escalated activities. Ensures continuous updates of the data loss prevention platform to drive down false positives as identified by investigation after action reviews. Reports identified gaps in process and procedures to appropriate leadership.				
Advises management on business decisions that may significantly affect university-wide or departmental operations, policies or procedures in support of the data protection and loss prevention programs. Maintains currency with any changes in legal, regulatory and technology environments which may affect operations. Ensures senior management and staff are informed of any changes and updates in a timely manner.				
Promotes an environment that fosters inclusive relationships and creates unbiased opportunities for contributions through ideas, words, and actions that uphold principles of the USC Code of Ethics. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations and publications. Attends meetings, seminars and conferences and maintains continuity of any required or desirable certifications, if applicable.				

Other Requirements

Essential:	Emergency Response/Recovery	Essential:	Mandated Reporter
	In the event of an emergency, the employee holding this position is required to “report to duty” in accordance with the university’s Emergency Operations Plan and/or the employee’s department’s emergency response and/or recovery plans. Familiarity with those plans and regular training to implement those plans is required. During or immediately following an emergency, the employee will be notified to assist in the emergency response		A mandated reporter who in his or her professional capacity has knowledge of, or reasonably suspects a person who is under the age of 18 years, elderly, or a dependent adult has been the victim of abuse or neglect must report the suspected incident. The reporter must contact a designated agency immediately or as soon as practically possible by telephone or in writing within 36 hours. By virtue of the associated job duties, this position qualifies as a mandated reporter as required by state law

Other Requirements

Essential:	*Emergency Response/Recovery*	*Essential:*	*Mandated Reporter*
	efforts, and mobilize other staff members if needed.		and USC's policy at: https://policy.usc.edu/mandated-reporters/

Campus Security Authority (CSA)	*Essential:*
By virtue of the associated job duties, this position qualifies as a Campus Security Authority as required by law and USC's policy at: https://dps.usc.edu/alerts/clery/	

ACKNOWLEDGMENTS

The above statements reflect the essential and non-essential functions as necessary to describe the principle contents of the job. They are not intended to be a complete statement of all work requirements or duties that may be required of the position. I understand that I may be asked to perform other duties as assigned. USC reserves the right to add or change duties at any time.

The University of Southern California is an Equal Opportunity Employer. USC prohibits discrimination on any basis protected under federal, state, or local law, regulation, or ordinance or university policies. All employment decisions are based on individual qualifications and business need.

I acknowledge receipt of this job description and its associated physical requirements. I have read and understand the job description and job requirements and agree to abide by their contents. I realize that duties may be requested of me that are not specifically stated herein. I understand that I will be expected to adjust to potential fluctuations in work volume. I understand that, if I have any questions about the essential functions or expectations of my position, my supervisor and/or HR partner are available to discuss them with me.

_____	_____	_____
Print Employee Name	Signature	Date
_____	_____	_____
Print Manager Name	Signature	Date

This job description describes the general nature and level of work required by the position. It is not intended to be an all-inclusive list of qualifications, skills,
duties, responsibilities or working conditions of the job. The job description is subject to change with or without notice, and Management reserves the right to add, modify or remove any qualification or duty. Nothing in this job description changes the existing at-will employment relationship between the university and the employee occupying the position.