Position Description

Position Description	
Report Run Date	Aug 30 2017 7:58PM
Position Number:	02021352
Dept:	ENT APPS & INFRASTRUCTURE SVCS - 061419
Position:	Senior Information Security Analyst
Approved Payroll Title Code:	0661
Approved Payroll Title:	IT SECURITY ANL 4
Approved MSP Salary Grade:	
Approved PSS Salary Grade:	MSP24
POSITION DETAILS	
Job Summary:	Under the general direction of the Assistant Chief Information Security Officer manage security and data protection solutions that support the mission of the university and protect the confidentiality, integrity, and availability of information assets owned or entrusted to UC Davis. Provides information security subject matter expertise to business and project teams to define security requirements for various technologies, performs vulnerability and risk assessments, determines deviations from acceptable configurations and University or department policy, creates and executes security governance, assists/performs forensics data collection and analysis, serves on the incident response team, provides log and vulnerability management expertise and operational duties as necessary, provides subject matter expertise in the information security domains to the organization, prepares/maintains various security reports and dashboards, coordinates technology audit activities, prepares and reviews system security architecture designs, actively participates with business and campus units throughout the university community, and plays an important role in the effort to secure the information assets of UCD from threats to the confidentiality, integrity, and availability of such assets. Tests, implements, deploys, maintains, reviews, monitor, and administers the infrastructure hardware and software that are required to effectively manage the campus vulnerability and log management resources. Responds to crisis or urgent situations within the University to mitigate immediate and potential threats. Stay abreast of evolving campus needs, technology capabilities, and threat intelligence from a variety of sources to optimize data protection measures. Works with campus stakeholders to ensure data security needs and controls are aligned to support organizational goals and objectives. Provides guidance on information security matters and proposes new services, standards, and operating procedures that enable the campus to effectively and efficiently address information security risks and comply with laws and regulations governing data protection. Tracks and reports on security risks and control effectiveness to the CISO and other campus stakeholders such as the Chief Information Officer, Network Operations Managers, security professionals located

	at the Davis and Sacramento campuses and other campus IT leaders. Operates with a degree of autonomy, uses independent thinking to creatively solve problems and issues, makes independent decisions, and must maintain or preserve confidentiality when required to do so.
Campus Job Scope:	
Department Specific Job Scope:	The Senior Network Security Analyst will mentor the junior members of the security team and create a positive environment where the junior members of the security team can enhance their skills as security professionals.
Positions Supervised:	N/A
Essential Responsibilities:	25% INFORMATION SECURITY CONSULTING -Provide information security subject matter expert consulting -Perform information security analysis & assessments on new systems, network devices, and applications with recommendations & assessment results provided to stakeholders. -Prepare new, and maintain existing, security assessment checklists and analysis documentation as required to ensure security assessments are reliable, efficient, and effective -Provide formal assessment reports to management including mitigation recommendations & status. 40% OPERATIONS -Provide technical security expertise and operational duties as necessary form many security systems and technologies including, but not limited to, the following: -Threat Intelligence solutions sponsored by the Office of the President -Intrusion Prevention Systems -Email Security tools -Firewalls and security appliances -VPN infrastructure -DMZ and Extranet infrastructures -802.11 Wireless networks -Security Information and Event Management system -Two-factor authentication system -Anti-malware technologies -Cryptography (Symmetric, Asymmetric, in transit, at rest) -Data Leakage/Loss Prevention -Provide timely detection, identification, and alerts of possible attacks/intrusions, anomalous activities, and misuse activities, and distinguish these incidents and events from benign activities -Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, & effects on system and information -Monitor external data sources (e.g., computer network defense vendor sites, Computer Emergency Response Teams, SANS) to maintain currency of network defense threat condition and determine which security issues may have an impact on the enterprise. Upon becoming aware of information security threats, assess & ensure departmental system administrators are aware in a timely manner of relevant threats to the associated systems they administer -Employ approved defense-in-depth principles & practices (e.g., defense-in-multiple places, layered defenses, security robustness) -Conduct/support authorized penetration testing on enterprise network assets -Assist with the selection of cost-effective security controls to mitigate risk (e.g.,

	protection of information, systems, & processes) -Lead security related projects -Maintain currency in languages, analytical techniques, and development methodologies. Learn new and emerging technologies by taking classes, attending conferences, and self-study. 10% NETWORK SECURITY & ARCHITECTURE DESIGN -Review, comment, and/or edit network & security architecture designs. -Perform/assist with design of system security architecture and controls to meet security objectives. -Perform, assist, and coordinate network penetration testing & provide formal assessment reports to management including mitigation recommendations and status. 10% INCIDENT RESPONSE -Serve as a member of the incident response team. -Perform/assist with forensic data collection & analysis. 15% DOCUMENTATION AND GOVERNANCE -Prepare, maintain, and review various security standards, guidelines, and policies. -Prepare/maintain measurement documentation including reports, dashboards, & other security related metrics or documents. -Develop/assist with the creation of formal request and procurement related documents such as RFPs, RFQs, Purchase Requests, and Response Scoring. -Assist with & perform duties required to set budget and acquire security technologies including obtaining quotes and assessing technologies and services to meet the business and security objectives. -Prepare corrective action responses to technology audit findings. -Participate in research of IT security tools, techniques, methodologies, technologies, and architectures -Participate on various security & technology related committees and workgroups.
Physical Demands:	
Work Environment:	-Work alternate or extended hours on short notice. -Occasional travel is required to campus and off campus worksites. -Due to the mission-critical services provided by this department, this position may work hours other than M-F 8-5, especially during system development, hardware or software installation, or in response to system problems. UC Davis is a smoke and tobacco free campus effective January 1, 2014. Smoking, the use of smokeless tobacco products, and the use of unregulated nicotine products (e-cigarettes) will be strictly prohibited on any UC Davis owned or leased property, indoors and outdoors, including parking lots and residential space.
Background Check:	Yes
QUALIFICATIONS	
Minimum Qualifications:	-Experience using computer network defense and vulnerability assessment tools, including open source tools, and the ability to transform output into complete professional reports. -Experience using intrusion detection methodologies and techniques for detecting

	host and network-based intrusions via intrusion detection technologies. -Experience with common security assessment and analysis tools (e.g., nmap, Nessus, TippingPoint, HP ArcSight, Fidelis, and FireEye) -Strong experience preferred with the security technologies such as SIEM, web application firewalls, VPN infrastructure, Intrusion Prevention Systems, DMZ and Extranet infrastructures, 802.11 Wireless networks, Multi-factor authentication, DNS, SMTP, FTP/SFTP, DHCP, 802.1x access control, Anti-malware, Data Leakage/Loss Prevention, switching and routing infrastructure and protocols. -Experience with Microsoft platforms (including Active Directory and Group Policy) and Unix/Linus OS X -Strong understanding of software/application/database security, system hardening, and secure code analysis (static/run-time) tools -Strong incident handling and forensics experience. -Understanding of cryptography, network hardening and secure networking principles. -Experience using host/network access controls (e.g., access control list) and network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS]). -Experience using information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation. -Expert knowledge of common network/data enumeration and attack methods. -Experience conducting vulnerability scans and recognizing vulnerabilities in security systems.
Preferred Qualifications for Selection:	-Strong information security policy, standards, and guidelines preparation and maintenance experience. -Strong information security metrics and status report preparation and maintenance experience. -Good project management skills. -Proven method to stay current on global threats and vulnerabilities. -Excellent time management skills and the ability to multi-task and work independently and consistency meet deadlines and expectations. -Experience communicating complex technical subjects in an understandable manner to both technical and non-technical audiences with tact and discretion. -Bachelor's degree in related area and/or equivalent experience/training. -Strong proficiency with common productivity software such as Microsoft Visio and Excel. -Extensive experience in an information security role in a University setting. -Strong knowledge of information security frameworks and standards such as ISO, NIST and regulations related to information security such as PCI, HIPAA, FISMA, SB 1386, etc., -Experience performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). -Experience using interpreted and compiled computer languages. -Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution). -CISSP, CISM, CISA or GIAC certifications.

Expectations	
Job Expectations	-Adhere to workplace safety practices, read information communicated about workplace safety, complete required safety training on time, report any workplace safety issues promptly to their supervisor or the designated safety coordinator. -Read and model the UC Davis Principles of Community -Communication skills to effectively present information (oral, written, presentation, documentation). -Use tact and diplomacy for interactions with others. -Communication skills to understandably and effectively describe technical

	requirements to technical and non-technical audiences. -Provide higher level technical assistance to the technical workforce in the resolution of abnormal operating conditions. -Support departmental goal of providing positive, innovative and effective customer service through performance of job functions. -Work cooperatively with others to achieve and maintain a strong client service environment. -Highly motivated and results orientated. -Maintain flexibility in a continuously changing and fast paced work environment. -Excellent organizational and analytical skills. -Ability to work independently under general direction from management, to manage workload across multiple simultaneous projects, to maintain a high level of productivity, and to meet deadlines under time constraints and continuously shifting priorities. -Maintain up-to-date knowledge through literature, classes, exhibits, seminars, on-the-job training and other relevant training forums. -Willingness to learn and apply new technology and willingness to develop skills to promote professional growth. -Willingness to routinely stay in communication with technical staff at other organizations to stay abreast of computing developments and resources available over the network. -Accountability for the safekeeping of resources in the employee's care and custody and for following and implementing the cyber-safety guidelines. -Work cooperatively and collaboratively with others in support of the mission of UCD. -Demonstrate flexibility and willingness to assist in other areas of the department when needed. -Ability to cultivate trust and build successful working relationships with stakeholders, subject matter experts, and other relevant staff and management. -Work with a diverse group of people in such a manner as to build high morale and group commitments to goals and objectives.