Security Analyst (0661U), Information Security Office - 65233
University of California, Berkeley

Direct Link: https://www.AcademicKeys.com/r?job=234765
Downloaded On: May. 16, 2024 4:40am
Posted Apr. 16, 2024, set to expire Jun. 30, 2024

Job Title	Security Analyst (0661U), Information Security Office - 65233
Department	
Institution	University of California, Berkeley Berkeley, California
Date Posted	Apr. 16, 2024
Application Deadline	Open until filled
Position Start Date	Available immediately
Job Categories	Professional Staff
Academic Field(s)	Information Technology
Apply Online Here	https://apptrkr.com/5184514
Apply By Email	
Job Description	

Image not found or type unknown

Security Analyst (0661U), Information Security Office - 65233

About Berkeley

At the University of California, Berkeley, we are committed to creating a community that fosters equity of experience and opportunity, and ensures that students, faculty, and staff of all backgrounds feel safe, welcome and included. Our culture of openness, freedom and belonging make it a special place for students, faculty and staff.

The University of California, Berkeley, is one of the world's leading institutions of higher education, distinguished by its combination of internationally recognized academic and research excellence; the transformative opportunity it provides to a large and diverse student body; its public mission and commitment to equity and social justice; and its roots in the California experience, animated by such values as innovation, questioning the status quo, and respect for the environment and nature. Since its founding in 1868, Berkeley has fueled a perpetual renaissance, generating unparalleled intellectual, economic and social value in California, the United States and the world.

We are looking for equity-minded applicants who represent the full diversity of California and who demonstrate a sensitivity to and understanding of the diverse academic, socioeconomic, cultural, disability, gender identity, sexual orientation, and ethnic backgrounds present in our community. When you join the team at Berkeley, you can expect to be part of an inclusive, innovative and equity-focused community that approaches higher education as a matter of social justice that requires broad collaboration among faculty, staff, students and community partners. In deciding whether to apply for a position at Berkeley, you are strongly encouraged to consider whether your values align with our Guiding Values and Principles, our Principles of Community, and our Strategic Plan.

At UC Berkeley, we believe that learning is a fundamental part of working, and our goal is for everyone on the Berkeley campus to feel supported and equipped to realize their full potential. We actively support this by providing all of our staff employees with at least 80 hours (10 days) of paid time per year to engage in professional development activities. To find out more about how you can grow your career at UC Berkeley, visit grow.berkeley.edu.

Departmental Overview

Berkeley IT believes in and fosters a workplace environment where people can bring their diverse skills, perspectives, and experiences toward achieving our goals through a process of critical inquiry, discovery, innovation, while simultaneously committing to making positive contributions towards the betterment of our world.

In addition, members of the Berkeley IT community have created and endorse the following values for our organization to augment and amplify the campus principles:

- We champion diversity.
- We act with integrity.
- We deliver.
- We innovate.

Diversity, Inclusion, and Belonging are more than just suggestions for us. They are the guiding principles underlying how we come together, develop leaders at all levels of the organization, and create an environment that unites us. We affirm the dignity of all individuals, call upon our leaders to address critical issues with integrity and intention, respect our differences as well as our commonalities, and strive to uphold a just community free from discrimination and hate.

Team Overview:

The Information Security Office (ISO) coordinates the risk management process for UC Berkeley's information systems and directs campus-wide efforts to adequately secure Institutional data. ISO is led by the Chief Information Security Officer and consists of seven areas: Information Security Policy, Information Security Operations, Information Security Development, Identity and Access Management, Information Security Assessments, Outreach and Engagement, and Service Management. This position is part of the Security Operations team and reports to the Information Security Operations Manager.

The Information Security Operations team is an inclusive group of talented professionals performing critical information security functions for the institution, including monitoring for intrusion, vulnerability scanning, incident/breach response, asset registration, designing and building security systems to help reduce risk, and the management of systems in support of these functions both on-premises and in multiple cloud environments.

Application Review Date

The First Review Date for this job is: Monday, April 29, 2024

Responsibilities

This position supports the activities of the Security Operations team as a Security Analyst, including security log/alert review, incident handling, security consulting, and architecture review. The successful candidate should have sufficient knowledge and experience to analyze and respond to security incidents of moderate scope and complexity, design and build security systems, and deploy commercial security tools and integrate with existing production operations.

Security Administration:

- Implement highly complex and broad-scale security controls to prevent unauthorized access or changes to campus hardware, software, and network infrastructure within systems such as Firewalls, intrusion detection/prevention systems (IDS/IPS), an Endpoint Detection and

Remediation system (EDR agents), and a Security Information and Event Management system (SIEM). These services provide security to all of UCB computers, networks, users, and information both on campus, in the cloud, and for remote workers.

- Provide research, analysis and solutions to address attempted efforts to compromise security protocols.
- Proactively addresses the negative impact on the campus caused by theft, destruction, alteration or denial of access of information.
- Advise the campus community on security prevention, best practices and secure software.
- Advise and recommend complex security controls that are broad in scope to prevent hackers from accessing critical information or jeopardizing the most sensitive systems both on-premises and in multiple cloud environments.
- Research and address attempted efforts to compromise endpoints using endpoint detection and remediation agents.
- Identify, develop, implement, and maintain complex campus-wide, and in multiple cloud environments, systems for the detection and identification of malicious activity using both intrusion detection and intrusion prevention systems.
- Research and analyze security alerts which may indicate efforts to compromise campus IT resources, and escalate alerts requiring further review by senior analysts.
- May lead a team of IT security professionals.

Event Management:

- Design and maintain highly complex security systems.
- Administer highly complex security policies and configurations to control access to hardware, software and networks. Applies and recommends highly advanced encryption methods.
- Identify, develop, and implement complex systems for the detection and identification of malicious activity both on-premises and in multiple cloud environments.
- Advise members of the campus community with general questions or concerns about the security configuration of campus IT systems

Forensics and Investigations:

- Directs forensic activity and produces reports in response to highly complex or broad-scale security incidents in accordance with the campus or Office of the President policy.
- Applies advanced IT security concepts, governmental regulations, departmental and campus, or Office of the President policies and procedures to provide input to, define or revise incident

response processes.
- Monitor security incident status and workflows, escalating unusual or problematic incidents to additional analysts for review and further action.
- Advise and provide leadership to campus IT personnel responding to security incidents on appropriate procedures and aid in the execution of incident response plans.
- Triage security incidents and support tickets on a periodic analyst rotation.
- Track and monitor incoming security incidents, applying security concepts and established campus procedures to ensure an appropriate incident response.
- Engages in continuous professional development and training.

Required Qualifications

- Minimum of 5 years of general IT knowledge and experience, including support, troubleshooting, and security best practices for a variety of desktop/server operating systems and software.
- Excellent communication skills, and ability to effectively communicate across a broad range of campus audiences.
- Strong interpersonal skills in order to work with both technical and non-technical personnel at various levels in the organization.
- Ability to serve as a lead for less experienced professionals on campus.
- Significant knowledge of key information security concepts, functions, and general best practices.
- Ability to understand different perspectives and cultures. Contributes to a work climate where differences are valued and supported.
- Demonstrated commitment to the advancement of diversity, equity, inclusion, belonging, justice and accessibility.

Preferred Qualifications

- Experience using an enterprise class SIEM tool such as ArcSight, Splunk, QRadar, Chronicle, or Elastic Security.
- Strong technologist with a pragmatic view and creative mind, and a natural collaborator with architects, engineers, developers, application owners, and service providers.
- Demonstrated ability to assume independent and team-based responsibilities while serving as

technical lead for engaging communities on information security issues in both on-premises and cloud environments.
- Experience working with and adapting common security policies, standards, and frameworks such as NIST 800-171, ISO 27001, CIS, and MITRE ATT&CK.
- Knowledge of Intrusion Detection, Firewall, Host, and Network Forensics.
- Experience in technologies such as SaaS, IaaS, PaaS, and other cloud environments with experience in the implementation of security architectures for cloud-native and hybrid cloud-based systems.
- Knowledge of Incident Handling Policies and Procedures.
- Ability to develop technical solutions to help mitigate observed security gaps and vulnerabilities.

Salary & Benefits

For information on the comprehensive benefits package offered by the University, please visit the University of California's Compensation & Benefitswebsite.

Under California law, the University of California, Berkeley is required to provide a reasonable estimate of the compensation range for this role and should not offer a salary outside of the range posted in this job announcement. This range takes into account the wide range of factors that are considered in making compensation decisions including but not limited to experience, skills, knowledge, abilities, education, licensure and certifications, analysis of internal equity, and other business and organizational needs. It is not typical for an individual to be offered a salary at or near the top of the range for a position. Salary offers are determined based on final candidate qualifications and experience.

The budgeted salary or hourly range that the University reasonably expects to pay for this position is $105,500.00 - $153,100.00.

- This is a 100%, full-time (40 hours per week), career position that is eligible for full UC benefits.
- This position is exempt and paid monthly.
- This position is eligible for flexible, hybrid or fully-remote work (telecommuting) based on candidate availability and business needs.

How to Apply

To apply, please submit your resume and cover letter.

AcademicKeys
UNLOCKING ACADEMIC CAREERS

Security Analyst (0661U), Information Security Office - 65233
University of California, Berkeley

Direct Link: https://www.AcademicKeys.com/r?job=234765
Downloaded On: May. 16, 2024 4:40am
Posted Apr. 16, 2024, set to expire Jun. 30, 2024

Conviction History Background

This is a designated position requiring fingerprinting and a background check due to the nature of the job responsibilities. Berkeley does hire people with conviction histories and reviews information received in the context of the job responsibilities. The University reserves the right to make employment contingent upon successful completion of the background check.

Other Information

Please note that while there are two positions listed on jobs.berkeley.edu (Security Analyst (0661U), Information Security Office - #65233 and Senior Security Analyst (0662U), Information Security Office - #65109), we will only be filling one position at a time. Applicants are encouraged to apply for the role that best aligns with their skills and experience.

Equal Employment Opportunity

The University of California is an Equal Opportunity/Affirmative Action Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, or protected veteran status. For more information about your rights as an applicant, please see the U.S. Equal Employment Opportunity Commission poster.

For the complete University of California nondiscrimination and affirmative action policy, please see the University of California Discrimination, Harassment, and Affirmative Action in the Workplacepolicy.

To apply, visit
https://careerspub.universityofcalifornia.edu/psp/ucb/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_APP_SCH

Security Analyst (0661U), Information Security Office - 65233
University of California, Berkeley

Direct Link: https://www.AcademicKeys.com/r?job=234765
Downloaded On: May. 16, 2024 4:40am
Posted Apr. 16, 2024, set to expire Jun. 30, 2024

Contact Information

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

Contact

N/A
University of California, Berkeley
,