Security Operations Center Analyst

HEJ higheredjobs.com/search/details.cfm

UNIVERSITY OF CENTRAL FLORIDA

Facilities and Business Operations:

The Facilities and Business Operations at UCF is dedicated to fostering a conducive educational environment for our faculty, staff, students, and the broader community. We are committed to excellence, providing unparalleled expertise, and maintaining a world-class standard in service.

Please visit us at: https://fs.ucf.edu/ or Facebook and Instagram: UCF Facilities

The Opportunity:

The Information Technology department within Facilities and Business Operations is seeking to hire four (4) Security Operations Center (SOC) Analysts. The Security Operations Center (SOC) Analysts are critical to safeguarding the university's academic, research, and administrative environments. SOC Analysts are responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats, ensuring continuous protection of institutional assets through 24/7 operations. Leveraging both traditional and AI-driven security technologies, this role strengthens the university's overall cyber defense posture.

Classification Title: Information Security Professional III

Responsibilities:

- Monitor SIEM, EDR, IDS/IPS, firewalls, and other security tools for alerts and anomalies.
- Perform initial triage and validation of security alerts to identify potential incidents.
- Conduct deep analysis of events using multiple data sources (e.g., SIEM logs, endpoint telemetry, network traffic).
- Lead investigations involving advanced persistent threats (APTs), insider threats, or multi-stage attacks.
- Perform root cause analysis and develop post-incident reports with tactical and strategic recommendations.

- Create and tune detection rules and automation workflows within SIEM and SOAR platforms.
- Monitor, detect, and analyze AI-driven attack techniques (e.g., prompt injection, data poisoning, model theft, adversarial input attacks).
- Evaluate and deploy AI-based security capabilities (e.g., anomaly detection models, LLM-based analysis tools) to enhance threat visibility.

Minimum Qualifications:

Bachelor's degree and 4 years of relevant experience; or High School Diploma (or equivalent) and 8 years of relevant work experience in lieu of degree or an equivalent combination of education and experience pursuant to Fla. Stat. 112.219(6).

Preferred Qualifications:

We welcome candidates with any of the following experience:

- 5+ years of operational cybersecurity experience, including work in a Security Operations Center (SOC), incident response, or similar security operations role.
- Hands-on experience with core SOC technologies, including: SIEM platforms (e.g., Splunk, QRadar, Microsoft Sentinel), SOAR tools for automation and orchestration, Endpoint detection and response (EDR) solutions, Network IDS/IPS technologies, and Firewall administration and enterprise log analysis.
- Experience developing and tuning detection capabilities, including writing correlation rules, alerts, and automated workflows within SIEM and SOAR environments.
- Scripting proficiency (e.g., Python, PowerShell, Bash) for automation, custom detections, data parsing, and enrichment.
- Knowledge of emerging AI-driven attack vectors, including prompt injection, adversarial machine learning techniques, data poisoning, and model extraction attacks.
- Experience deploying or tuning AI-based security capabilities, such as anomaly detection models, AI-assisted triage tools, or LLM-driven threat analysis workflows.
- Demonstrated incident response expertise, including triage, advanced threat analysis, containment, root-cause analysis, and post-incident reporting.
- Familiarity with digital forensics tools, methodologies, and evidence-handling (endpoint, network, or cloud forensics).

- Understanding of cloud security principles and monitoring within Azure, Amazon Web Services (AWS), and/or Google Cloud environments, including hybrid infrastructure.
- Strong analytical, investigative, and problem-solving skills, with the ability to communicate technical findings clearly to both technical and non-technical audiences.
- Experience in higher-education or complex enterprise environments, including research and administrative support, data-security compliance frameworks (e.g., FERPA, HIPAA, NIST 800-171), and the unique network/security challenges of university settings.
- Relevant Industry-recognized certifications such as CompTIA Security+, CySA+, CEH, GIAC Security Essentials (GSEC), or Certified SOC Analyst (CSA).

Special Instructions to the Applicants:

The Security Operations Center (SOC) is open 24 hours per day, 7 days per week, including holidays. The SOC staff will work a rotational shift model to support continuous security monitoring. The selected candidate will be required to work rotating shifts that include nights, weekends, and holidays.

Position requires a valid Class E driver's license. This position may involve driving to various locations on and off campus to conduct University business.

Applicant must be authorized to work for any U.S. employer, as sponsorship is not available for this position now or in the future.

The anticipated salary range for this position is $89,076 to $100,000 The final salary will be determined based on the candidate's qualifications, experience, and internal equity considerations

If you are selected as the final candidate for an employment opportunity, both your position and salary will be significantly based upon the information that you have provided in your application for employment. We urge you to please take the time to complete the application in its entirety.

UCF is seeking to fill multiple roles. Candidates for this job posting will be considered for additional vacancies in this department.

Classification Title: Information Security Professional III

Are you ready to unleash YOUR potential?

As a next-generation public research university and Forbes-ranked top employer in Florida, we are a community of thinkers, doers, creators, innovators, healers, and leaders striving to create broader prosperity and help shape a better future. No matter what your role is, when you join Knight Nation, you'll play an integral role at one of the most impactful universities in the country. You'll be met with opportunities to connect and collaborate with talented faculty, staff, and students across 13 colleges and multiple campuses, engaging in impactful work that makes a positive difference. Your time at UCF will provide you with many meaningful opportunities to grow, you'll work alongside talented colleagues on complex projects that will challenge you and help you gain new skills, and you'll have countless rewarding experiences that go well beyond a paycheck.

Working at UCF has its perks! UCF offers:

- Benefit packages, including Medical, Dental, Vision, Life Insurance, Flexible Spending, and Employee Assistance Program
- Paid time off, including annual and sick time off and paid holidays
- Retirement savings options
- Employee discounts, including tickets to many Orlando attractions
- Education assistance
- And more...For more benefits information, view the UCF Employee Benefits Guide.

Dive into our Total Rewards Calculator to discover the diverse selection available to you, giving you a glimpse into the benefits that together shape your comprehensive rewards package at UCF.

Unless explicitly stated on the job posting, it is UCF's expectation that an employee of UCF will reside in Florida as of the date the employment begins.

Department

UCF IT Information Security Office

Work Schedule

UCF business hours are Monday-Friday 8:00 AM to 5:00 PM. The Security Operations Center (SOC) is open 24 hours per day, 7 days per week, including holidays. The SOC staff will work a rotational shift model to support continuous security monitoring. The selected candidate will be required to work rotating shifts that include nights, weekends, and holidays.

Type of Appointment

Regular

Expected Salary

$89,076.00 to Negotiable

Job Posting End Date

02-07-2026-12-00-AM

As a Florida public university, the University of Central Florida makes all application materials and selection procedures available to the public upon request.

UCF is proud to be a smoke-free campus and an E-Verify employer.

If an accommodation due to a disability is needed to apply for this position, please call 407-823-1336 or email onac@ucf.edu.

For general application or posting questions, please email talent@ucf.edu.
Your assistance with the University of Central Florida's Affirmative Action Plan implementation is appreciated. The University collects VOLUNTARY declarations of race and gender and uses the information to compile statistics on recruitment success. If you choose to assist, your demographic information will be used only for affirmative action. The University of Central Florida is an equal opportunity, equal access, and affirmative action employer.