The University of Texas at San Antonio

Job Description

Job Title:	Cybersecurity Operations Analyst
Code:	19245
Salary Grade:	60
FLSA Status:	Exempt
Department/Division:	Cyber Operations/University Technology Solutions
Reports To:	UTS Resource Manager – CyberSecurity Operations

Summary

Function:
To perform analyst duties within the Cybersecurity Operations Center (CSOC) and continually improve the Cybersecurity Operations program.

Duties

Typical:

1. Monitor and analyze logs and alerts from a variety of different technologies across multiple platforms in order to identify and mitigate incidents. This includes analysis of logs from: IDS/IPS, firewall, proxies, anti-virus and end-point protection, servers and workstations and other security technologies and devices.
2. Assess the security impact of security alerts and traffic anomalies to identify malicious activities and take mitigating actions or escalates to senior members of team as appropriate.
3. Leverage fundamental understanding of Operations Systems (Windows, Unix/Linus and OSX) in support of identifying security incidents and to have a proper overview of risk profile.
4. Execute analysis of email based threats to include understanding of email communications, platforms, headers, transactions and identification of malicious tactics, techniques and procedures.
5. Utilize and adhere to defined workflow and processes driving threat monitoring and escalation/handoff actions.
6. Document results of cyber threat analysis effectively and prepare comprehensive handoff and/or escalation as appropriate.
7. Create and utilize playbooks, standards and procedures.
8. Write reports.
9. Provide scripting capabilities.
10. Participate in appropriate opportunities for continuing education, seminars, organizations, etc.
11. Work Cybersecurity Operations tickets.
12. Perform other duties as assigned.

Education

Required	Preferred
Bachelor's degree from an accredited institution in cybersecurity, computer science, engineering or related field.	N/A

Other Requirements

Required	Preferred
Competency in common operating systems (e.g. Windows, macOS, Linux).	Individual technical Cyber Security Certification through a recognized body, CompTIA's Security+ or higher preferred, within 180 days of obtaining position.
Knowledge of networking concepts.	
Strong analytical skills.	
Excellent verbal and written communication skills.	
Ability to work both independently and collaboratively.	
Ability to work in a fast paced environment.	
Ability to communicate technical concepts to a non-technical audience.	
Ability to work remotely, with or without others, take direction and be a self-starter that take initiative.	
Excellent organization, problem resolution and teamwork skills.	

Experience

Required	Preferred
None.	One year of related experience.
	One year of experience or academic equivalent in scripting/programming languages such as Python or PowerShell.

Equipment

Required	Possible
Personal computers, Microsoft Office and standard office equipment.	N/A

Working Conditions

Usual	Special
Work requires flexibility of hours to include evenings and weekends as needed.	Occasional travel may be required.

Supervision

Received	Given
General supervision from assigned supervisor.	N/A

Accuracy

Proficiency in all phases of the duties performed.

Security Sensitive

Specific job requirements or physical location of some positions allocated to this classification may render the position security sensitive, and thereby subject to the provisions of section 51.215 Texas Education Code.

Internal Control

Within the scope of position duties, responsible for seeing that operations are effective and efficient, assets are safeguarded, reliable financial data is maintained, and applicable laws, regulations, policies, and procedures are complied with.