Job Code: 101602
Position #: (PSA).....(E)
Developed by:..... MK
Reviewed by:..... DLJ
Approved by:.....LK
Date: 10/03/22

UNIVERSITY OF RHODE ISLAND
Position Description

TITLE: Cybersecurity Threat Analyst

DIVISION: Academic Affairs / Administration and Finance (ITS)

REPORTS TO: Chief Information Security Officer

GRADE 14

SUPERVISES: Technical staff

BASIC FUNCTION:

Under the direction of the Chief Information Security Officer within the Office of Information Technology Services, work closely with the IT Security Services team to perform IT security analysis and assessments in accordance with established procedures and protocols. Ensure the demonstrable Confidentiality, Integrity, and Availability (CIA) of the University of Rhode Island's information assets for authorized internal and external users by reviewing, validating, classifying, and responding to security events and cyber-attacks. Utilize best practices, risk management techniques, critical thinking, strong analytical skills, and incorporated knowledge to detect, assess, and respond to cybersecurity events and incidents across URI networks. Manage tasks that may be part of audit support functions as they relate to the impact and importance of legal and regulatory compliance.

Maintain primary focus on proactively seeking out indicators of compromise that conventional cybersecurity processes cannot find, and threats and campaigns aimed at the University. Work with IT Security Services team members as well as application owners to identify and mitigate security threats to applications identified through testing. Communicate with business process owners, application owners, IT staff and development partners. Interact closely with product vendors and service providers, with personnel from various IT departments — including IT Teaching and Learning Services (ITTLS), IT Research Computing Services (ITRCS), IT Administrative Services (ITAS), IT Community Services (ITCS), IT Infrastructure Services (ITIS), IT Innovation (ITI), IT Service Administration (ITSA — and with distributed ITS Partners and business units across the university.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

Test the effectiveness and resiliency of the university's information systems and infrastructure by identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Enhance and improve testing tools, scripts and methodologies as needed.

Lead in all scoping, scheduling, and logistics for each penetration test and security assessment.

Communicate and coordinate activities with product owners and assure that priorities are developed and known.

Ensure a successful defensive security posture for the university by leveraging effective policies and governance, strong technical defenses, combined with appropriate action from people.

Design, maintain, and enhance testing scripts, tools, and processes.

Continually improve application security assessment processes to keep up with the industry standard methodologies.

Provide leadership in penetration testing service offering.

Maintain an overall inventory of applications, owners, and testing results.

Collate security incident and event data to produce monthly exception and management reports.

Manage the log analysis platforms, including but not limited to performance tuning and application maintenance.

Work hands-on with data to collect, summarize, and visualize operational metrics based on detailed log data in support of IT activities.

Build, maintain and improve dashboards to describe past, present, and future trends.

Work with ITS and partners to establish processes for adding resources and groups to the shared log analysis environment.

Identify opportunities to improve institutional systems, processes, and data.

Support log ingestion from a variety of sources into the enterprise log analysis infrastructure.

OTHER DUTIES AND RESPONSIBILITIES:

Participate in business continuity and disaster recovery planning.

Create and maintain a complex variety of security and risk documentation (e.g., Policies, process diagrams, risk registers, etc.) that may be shared with various audiences.

Assist in cultivating a risk aware culture through outreach and education.

Perform other duties as assigned.

LICENSES, TOOLS, AND EQUIPMENT:

Highly specialized knowledge of a specific technology; Microsoft Office Suite (advanced Excel skills: information security concepts, relevant tools, and standards; advanced Information Security principles.

ENVIRONMENTAL CONDITIONS:

This position is not substantially exposed to adverse environmental conditions.

QUALIFICATIONS:

REQUIRED: Bachelor's degree; Minimum five years of progressively responsible experience working in information technology, security, and/or risk management; Demonstrated understanding of OWASP, SANS, PTES frameworks and common vulnerabilities, and attack vectors; Demonstrated experience with port, protocol, and service enumeration (e.g., Wireshark, Rumble, Nmap, and Massscan); Demonstrated experience with Vulnerability scanning (e.g., Qualys); Demonstrated experience with web and mobile application testing; Demonstrated experience with log aggregation and analytics platforms (e.g., Splunk, Apache Spark or ELK); Demonstrated technical experience with application performance tuning, log ingestion, and general administration of the aforementioned applications; Demonstrated experience working with one or more scripting languages (especially Python) and one or more cloud providers (Azure, AWS, OCI); Demonstrated experience with GIT workflow and version control systems; Demonstrated strong verbal and interpersonal communication skills; Demonstrated proficiency in written communication skills; Demonstrated ability to manage multiple, competing priorities and develop potential solutions in a deadline-driven environment; Demonstrated knowledge and understanding of information security industry standards and government regulations; and, Demonstrated ability to work with diverse groups/populations.

PREFERRED: Certifications inclusive of log analysis products or approaches, i.e., CEH (Certified Ethical Hacker); Minimum three years of information security experience; Minimum three years of experience in log analytics, systems administration, etc.; Minimum two years of Application Security Testing Experience; Minimum two years of Information Security penetration tools experience; and, Demonstrated experience working within Higher Education.

ALL REQUIREMENTS ARE SUBJECT TO POSSIBLE MODIFICATION TO REASONABLY ACCOMMODATE INDIVIDUALS WITH DISABILITIES.