THE UNIVERSITY OF THE WEST INDIES DIGITAL TRANSFORMATION PROJECT

TERMS OF REFERENCE

CONSULTANCY SERVICES FOR DELIVERY OF TRAINING IN CYBERSECURITY

BACKGROUND

The University of the West Indies (UWI) has requested assistance from the Caribbean Development Bank (CDB) in financing training to harden and improve the institution's Cybersecurity posture. UWI's has established a Computer Security Incident Response Team (CSIRT) across five (5) campuses and seeks financing training with the aim of addressing prioritized deficits across the campuses in the area of cybersecurity.

The consultancy is for the delivery of training with the aim of acquiring requisite skills to securely administer UWI's security fabric and ecosystem in the Cybersecurity realm.

OBJECTIVES OF THE COMPONENTS

The objective of the Components is to provide comprehensive training for the UWI CSIRT in targeted areas of interest identified and to deliver these instructor-led sessions. These sessions should be in alignment with University's move to improve staff members' competencies, and to effectively deal with threats, such as, zero-day attacks, and manage emerging technologies, primarily, cloud computing. Additionally, and importantly, the training is expected to buttress UWI's capability to protect its informational assets and supporting infrastructure.

The instructor-led training will consist of the following components:

Course
Certified Ethical Hacking Certification
CompTIA Security+ Certification
Security Information and Event Management (SIEM)
Certified Information Systems Security Professional (CISSP) Certification

SCOPE OF SERVICES

The scope will include training for members of the UWI CSIRT in a hybrid mode, incorporating both theoretical and practical sessions. It is desirable to train all the members of the Team in the above listed areas, however, this is contingent on the associated costs. Given the breadth of the

above-mentioned Components, the situation may arise in which more than one (1) consultant is engaged to provide the respective training in a particular area.

As part of the fulfilment of these Components, the Consultant(s) shall deliver the following services, based on a schedule to be established:

a. Prepare and facilitate lessons on topics identified
b. Prepare training schedules.
c. Provide supporting materials to participants, electronically, otherwise.
d. Conduct an evaluation of the training and provide a report to the Programme Coordinator.
e. Provide reports on students' performance and progress.
f. Report any problems, incidents and concerns relating to the programme.
g. Work with the Programme Coordinator to deliver appropriate practical activities to engage the participants.
h. Perform other related work as required

SUMMARY DESCRIPTION OF COURSES

The IT Security landscape has changed and continues the rapidly change as threat actors become more sophisticated, targeting a wider range of informational assets across the world. The knowledge required years ago is no longer adequate to protect an institution of the present.

Universities are not excluded from the list of prime targets and information security has now been thrusted to the apex of priorities for CIO's and institutions. IT Security staff must now be adequately equipped with the requisite knowledge, complimented by practical hands-on skills to meet the new challenges in this arena. It is thus paramount for UWI's IT Security staff to be effectively and adequately trained.

Some of the required courses include:

Certified Ethical Hacking Certification (CEH)

- Participants will be trained with a view to enhance their skills in systematically assessing network infrastructures to find security vulnerabilities which a malicious hacker could potentially exploit.

The content of the course will incorporate:

- Creating perimeter defenses,
- Scanning and attacking networks,
- Escalating privileges,
- Intrusion detection,
- Policy creation,
- Attack Methodologies - *Social engineering, DDoS attacks, buffer overflows and virus creation*

CompTIA Security+ Certification

- Participants are expected to acquire core knowledge required of any cybersecurity role and to operate at operational level within the cybersecurity realm. The course incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:
- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, and IoT.
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

Security Information and Event Management (SIEM)

- Participants are expected to acquire core knowledge to detect, analyze, and respond to security threats before they harm business operations. It includes the collection of event log data from a range of sources, identifying activity that deviates from the norm with real-time analysis, and taking appropriate action. The course will incorporate:

- Building and designing multi-tenancy SIEM Architecture.
- Collecting data / logs from any data sources (Cloud, Hybrid, On-Premise).
- Leveraging AI & ML (Machines Learning Models) for detection.
- Building custom detection & analytics rules.
- Building automation rules and playbooks for custom integration and/or response and remediation

Certified Information Systems Security Professional (*CISSP)* Training

Certified Information Systems Security Professional (*CISSP)*, is a certification for advanced IT professionals who want to demonstrate that they can design, implement, and manage a cybersecurity program at the enterprise level. It is commonly referred as the “Gold Standard of IT Security Certification”.

Participants will be trained in areas which will provide the technical and managerial competence required from an experienced information security professional to effectively design, engineer, implement and manage an organization's cybersecurity program within an ever-changing security landscape.

The subject matter that the CISSP certification covers is broken down into eight areas, called domains.

These domains include:

- ✓ *Security and risk management*
- ✓ *Asset security*
- ✓ *Security architecture and engineering*
- ✓ *Communication and network security*
- ✓ *Identity and access management (IAM)*
- ✓ *Security assessment and testing*
- ✓ *Security operations*
- ✓ *Software development security*

QUALIFICATION AND EXPERIENCE

The Consultant(s) must have strong inter-personal skills with a proven ability to work cooperatively with diverse groups and stakeholders and should possess the following minimum qualifications:

- Industry-recognized certification in the respective area of training.
- Minimum of five years in the respective area of IT Security.
- Minimum of five years in a teaching/learning environment.
- Strong spoken and written communication skills and fluency in the English language.

DURATION

Each component will be delivered over a maximum of five (5) days per week, with the total duration being 4 weeks.

Date Last Modified: July 17, 2023