STATE OF WASHINGTON
EDMONDS COLLEGE
SOLE SOURCE POSTING

May 5, 2023

EDMONDS COLLEGE contemplates awarding a sole source contract to CYBER RANGES Corporation to provide a safe and legal environment with simulated representations of networks, systems, tools, and applications. This domain will allow students to gain hands-on cyber skills and provide a secure environment for product development and security-posture testing.

EDMONDS COLLEGE requires a cloud-based educational platform that integrates actual hardware and software, while supporting a combination of physical and virtual components. This environment will play a central role in facilitating and fostering cybersecurity education, training, and certification.

EDMONDS COLLEGE will enter into a THREE (3) YEAR contract with CYBER RANGES Corporation. The contract will be issued on or after MAY 23, 2023 and will continue for a THREE year term. The cost of this THREE year contract is $403,690.

Offerors contemplating the above requirements are required to submit capability statements detailing their ability to meet the state's requirements within five (5) working days of this announcement.

Capability statements should address the following state requirements:

- 24x7 availability.
- 100% cloud based.
- Cyber range connectivity capability via a Virtual Private Network (VPN) connection.
- Integration capable with the Canvas learning management system (LMS).

STUDENT EXERCISES/PLAYLISTS/SCENARIOS/EDUCATIONAL CONTENT THAT:

- Maps to well-known and accepted cybersecurity standards, to include the NIST Cyber Security Framework, ISA/IEC 62443, ISO/IEC 27001, NIST SP 800-53, Center for Internet Security Critical Security Controls, and COBIT 5.
- Align with the Cyberspace Workforce Management DOD Directive (DoDD) 8140.
- Align with the MITRE ATT&CK Defender™ (MAD) training and credentialing program.
- Address the knowledge and skills needed for the Security Operations Center (SOC) Analyst, Penetration Tester, and Malware Analyst career paths.

OBSERVER FUNCTION/ROLE - FOR EACH PARTICIPANT/STUDENT, THE CAPABILITY TO:

- View their remote desktop.
- Control all the virtual machines, to include reboots and resets.
- Dynamically modify and add tasks and questions.
- Control the execution of injections.
- Control participation - suspend and remove.

ATTACK SIMULATION - FOR EACH PARTICIPANT/STUDENT, THE CAPABILITY TO:

- Configure the timing, number of injections, randomness, and IP addresses.
- Have observers execute attacks of their choice from exiting collections, or create their own.

SCENARIO CREATION/SCENARIO COMPOSER. THE CAPABILITY TO:

- Clone and repurpose both the scenarios and the simulation environments.
- Configure ACLs for group scenarios.
- Create theoretical scenarios, simulation environments (virtual infrastructures) and blue-team scenarios with automated attacks.
- Select from existing or pre-configured libraries for VMs, Networks, Assessments and Injections.

PARTICIPANT/STUDENT ASSESSMENT. THE CAPABILITY TO:

- Create the same question types that are supported by the Canvas learning management system. At a minimum: Essay, file upload, matching, multiple choice, and true/false.
- Map questions to the NIST NICE competency framework.

CONCURRENT USE SUPPORT FOR:

- Capture The Flag (CTF) events.
- Delivery of regularly scheduled classes in separate cyber range environments.
- Multiple participants/students engaged in self-paced study and/or research.

MULTI-PARTICIPANT EVENT SUPPORT. THE CAPABILITY TO CONFIGURE:

- Duration.
- Late registration or joins.
- Number of users.
- Password protection.
- Public/private events.
- Start date/time.

SUPPORT FOR CTI BASED ATTACKS ON OPERATIONAL TECHNOLOGY INFRASTRUCTURES:

- The ability to simulate cyber threat intelligence (CTI) based attacks on operational technology (OT) infrastructures such as those found in power substations, water systems, and gas plants. At a minimum, the simulations must be able to address:
- Distributed control systems (DCS).
- Human machine interfaces (HMIs).
- Industrial control systems (ICS).
- Industrial internet of things (IIoT) devices, aka Industry 4.0.
- Internet of things (IoT) devices.
- Supervisory control and data acquisition system (SCADA).

In the absence of other qualified sources, it is the state's intent to make a sole source award ofthe contract. To submit capability statements or for questions, contact:

Name: Kelvin Nesvog
Phone: 425.640.1586
Email: kelvin.nesvog@edmonds.edu