Maine's Public Universities
UNIVERSITY OF MAINE SYSTEM

REQUEST FOR PROPOSALS # 2025-055
Room Modeling and ECommerce Solution
RESPONSE ADDENDUM #1
February 20, 2025

QUESTIONS

1. **How many faculty and Students are expected in a year to get trained and use the cyber security solution?**

   ANSWER:

   We anticipate that four faculty members will receive training and utilize the cybersecurity solution each year. In addition, up to 200 students are expected to participate annually. The student number will vary depending upon what specific course will be offered in any given semester.

2. **Are there any existing SIEM, IDS, or firewalls the University expects the platform to integrate with? If so, what are the preferred vendors or technologies?**

   ANSWER:

   We currently prefer to integrate with Splunk or QRadar for SIEM, Snort for IDS, and Palo Alto for firewalls. However, we are open to other comparable, up-to-date solutions that align with our technology requirements.

3. **Does the University have a preferred ticketing or communication system for integration (e.g., ServiceNow, Slack, Discord, Microsoft Teams)?**

   ANSWER:

   We do not have a strict preference for a specific ticketing or communication system. However, our primary requirement is that the ticketing system be integrated into the training platform to streamline support and communication.

4. **Will the University accept pre-configured cyber scenarios that can be modified within defined parameters, or does it require full scenario creation capabilities?**

   ANSWER:

   We welcome the inclusion of preconfigured cyber scenarios that can be adapted to our specific needs, and we also require the capability to create fully customized scenarios for more specialized training.

5. **The RFP mentions a need for OT/ICS/SCADA simulations—can the University provide specific use cases or scenarios it envisions for this requirement?**

ANSWER:

We require OT/ICS simulations focusing on three primary domains—power distribution, water/wastewater systems, and smart manufacturing/IIoT. Specifically, we are looking for:

a. **Power Distribution:** Scenarios emulating SCADA-based breaker manipulation in power substations.
b. **Water/Wastewater:** Scenarios depicting PLC tampering in water treatment processes.
c. **Smart Manufacturing:** Scenarios illustrating HMI compromise within Industry 4.0/IIoT environments.

These simulations should include realistic data flows, adversary tactics, and must be customizable to reflect real-world conditions and evolving threats.

6. **Does the University require custom toolset configurations per user or per course, or will a standard set of cybersecurity tools suffice?**

ANSWER:

The University prefers a standard, comprehensive cybersecurity toolset that includes network monitoring/forensics, offensive security, digital forensics, incident response (DFIR), threat intelligence, ICS/OT scanning/security, and penetration testing. While a standard configuration is our primary focus, it should be flexible enough to cover the breadth of our courses and users.

7. **What level of traffic simulation customization is required? Would a pre-built malicious traffic sandbox meet this need, or does UMA require the ability to inject custom traffic into labs?**

ANSWER:

We require a solution that can generate realistic network traffic in each scenario, with the flexibility to inject custom traffic as needed. Additionally, we need the ability to adjust

overall traffic flow to simulate the challenge of distinguishing malicious traffic more closely from normal network behavior.

8. **The University requests "custom scripts and traffic integration"—is this referring to externally developed scripts, or is the expectation that the vendor provides scripting flexibility within the environment?**

ANSWER:

The University expects the vendor to supply scripts within the environment and support the integration of externally developed scripts. This approach ensures flexibility for both vendor-provided and custom solutions, enabling a more comprehensive testing experience.

9. **Would UMA prefer pre-set learning paths mapped to industry frameworks (e.g., NICE, DCWF/8140), or does it require the ability to define new paths from scratch fully? Would both be ideal?**

ANSWER:

The University would like the option to use pre-set learning paths mapped to recognized industry frameworks (e.g., NICE, DCWF/8140, NIST, Att&ck), while also retaining the flexibility to create entirely new learning paths from scratch. Having both options provides the adaptability we need to meet diverse training requirements.

10. **The RFP references hardware-in-the-loop integration—does UMA expect direct integration with specific physical appliances, or is a virtual emulation of hardware acceptable?**

ANSWER:

The University requires the capability to integrate physical hardware directly into the environment to replicate real-world conditions and accurately assess system performance in operational scenarios.

11. **What response time expectations does UMA have for technical support and issue resolution under the SLA?**

ANSWER:

UMA has outlined the following support and resolution expectations under the SLA:

a. **Critical (e.g., System Outages)**
    a. Response Time: Within 1 hour
    b. Resolution Time: 4–8 hours
b. **High-Priority**
    a. Response Time: 1–4 hours
    b. Resolution Time: 12–24 hours
c. **Medium-Priority**
    a. Response Time: Within 24 hours
    b. Resolution Time: 3–5 business days
d. **Low-Priority**
    a. Response Time: Within 48 hours
    b. Resolution Time: Dependent on complexity

12. **Does UMA require real-time reporting dashboards for instructors and administrators, or would scheduled reports be sufficient?**

    ANSWER:

    We require real-time reporting dashboards that can be customized to address our specific training objectives. In addition, we would like pre-built, standard reports available for on-demand access, ensuring quick insights into user progress and overall platform activity.

13. **Can you provide an approximate budget ceiling or funding source for this procurement?**

    ANSWER:

    We are seeking an affordable option(s) to meet the program needs.

14. **For a single license that can cover all three requirements, what is the preferred method of pricing across the three requirements?**

    ANSWER:
    Three (3) solutions are: Range, Cloud Based Labs and Organizational Exercises

    Refer to RFP Submissions Form Package, Appendix C, Exhibit 1, Table 1 and Appendix C, Exhibit 1, Table 3.
    Additionally please see instructions in RFP Section 1.1.3