AIR FORCE CYBERWORX™

Timeline:

Next AMA: May 22nd
Applications Open: May 28th
Applications Close: June 25th

To Apply:

https://afwerx.com/divisions/ventures/specific-topic/

Questions or to discuss more:

sbir.sttr@afcyberworx.org

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-0801: AI/ML - GENERATED DECOY NETWORKS

What is the end goal of this effort - operational deployment or experimental use?

The ultimate objective is operational deployment. While Phase I centers on feasibility, the desired outcome is a deployable system that functions within active defensive cyber operations. The decoy network should lure adversaries away from operational systems into high-fidelity, dynamic environments. These environments must also support persistent monitoring to gather actionable intelligence on adversary behavior and tactics. Solutions should be designed with real-world scalability, integration potential, and mission relevance in mind.

What level of realism and adaptability is expected in the decoy environment?

Realism is critical. The decoy must continuously evolve to remain believable under scrutiny from state-sponsored adversaries. This includes realistic user behavior, data flows, services, and infrastructure. The environment should appear valuable and exploitable—enticing enough to capture attention—but not so vulnerable or static that it is easily identified as a trap. AI/ML should be leveraged to monitor real or simulated networks and adapt the decoy in real time or through retraining. A well-calibrated balance of authenticity and stealth is essential for long-term deception.

What role should AI/ML play in the proposed solution?

AI/ML is expected to be central to the system's design. It should be used to learn from live, synthetic, or simulated network data—capturing behaviors, services, and traffic patterns—and generating decoy environments that mirror those observations. Additionally, AI/ML should drive adaptation over time, model user and adversary interactions, and detect intrusions or behavioral shifts. The solution should support autonomous updates and behavior generation while providing defenders with real-time insights into threat activity.

AIR FORCE CYBERWORX™

Timeline:

Next AMA: May 22nd
Applications Open: May 28th
Applications Close: June 25th

To Apply:

https://afwerx.com/divisions/ventures/specific-topic/

Questions or to discuss more:

sbir.sttr@afcyberworx.org

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-0801: AI/ML - GENERATED DECOY NETWORKS

What operational modes and response capabilities should the system support?

The system must support fully autonomous, semi-automated, and manual control modes. Autonomous operation ensures persistent deception with minimal operator overhead. Semi-automated and manual controls enable tailored intervention during targeted threat tracking. The system should be capable of real-time response to adversary behavior—modifying topology, adjusting services, or escalating alerts as needed. This responsiveness increases the credibility of the decoy while enhancing operator situational awareness.

Are specific architectures, technologies, or protocols required?

No specific architecture is mandated. Offerors may use AI/ML, expert systems, virtualization, containerization, or hybrid approaches. The key requirement is a flexible, scalable system that can emulate real operational environments across a range of protocols (e.g., HTTP, MQTT, MODBUS, DNP3) and behaviors. The architecture should allow for realistic traffic and service emulation, seamless integration of learning pipelines, and continuous refinement based on observed inputs.

What deployment environments and integration considerations should be anticipated?

The system should be designed for deployment in a range of environments, including secure cloud, on-premises, or hybrid configurations. A FedRAMP-approved cloud is not required, but cybersecurity best practices and modular design are essential. Solutions should be aligned with long-term integration pathways, including Risk Management Framework (RMF) compliance and Authority to Operate (ATO) readiness. Flexibility, portability, and ease of deployment will be critical for successful transition to operational environments.