Updated: 09-30-2024

BIRD Cyber 2024
Explanation of Topics

Topic	Description
1. Cyber Protection for Legacy Medical Devices	Legacy medical devices were designed and manufactured before awareness of cyber threats became commonplace. These devices can be difficult to update or replace. This topic seeks the development and demonstration of a solution that will protect a legacy device from cyber-attacks. The system will function as a smart mediator between the medical device and the network it is connected to, while not affecting its usual function or requiring any changes to the device itself. The project should end with a demonstration of the solution on an authentic legacy medical device in a controlled environment.
2. BGP Hijacking Remediation	Border Gateway Protocol (BGP) routing manipulation is a significant cybersecurity threat that may lead to many types of denial of service (DoS) and man-in-the-middle (MITM) attacks. Although solutions have been proposed to address these risks, they are complicated to implement and cover only some of the scenarios, so their global deployment is slow and insufficient. In addition, existing solutions for detecting and alerting of such manipulations do not provide an effective means for fast remediation. The proposed solution shall provide a system for automatic detection and fast remediation of hijacked BGP routes. The project shall conclude with a demonstration of the detection solution, and for the remediation aspect, the solution should be demonstrated at least in a lab or preferably as a beta site in a production environment.
3. Online Face Image Self-Enrollment Compatible with International Standards	As many countries, including the United States and Israel, move toward online passport renewal, one of the operational challenges concerns the ability to enroll a facial image, especially images taken as “selfies,” that meets quality standards of the International Civil Aviation Organization (ICAO) and/or American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) Type 10. Meeting the criteria for "selfies" would also enable a wider range of "liveness" detection methods that can be accessed when using the front camera of a smartphone. The proposed solution should provide a secure tool for self-enrolling an image that complies with the ICAO and/or ANSI/NIST standards for properties such as size, position, lighting, and background. Potential approaches could include: 1. Developing an AI tool for processing the image according to ICAO and/or ANSI/NIST requirements. 2. Combining a presentation attack detection system with a deep fake detection system. The project shall conclude with a demonstration of the solution and how it meets the required standards.

4. Threat Hunting on Encrypted Traffic	Threat Hunting teams perform in-depth investigations on network traffic using sensors deployed in the organization. In many cases the traffic is encrypted and there is no ability to verify whether the data is legitimate or malicious. The capabilities that will be developed as part of this project should allow identifying malicious activity in encrypted traffic without decrypting it. Potential approaches may include (but are not limited to): 1. Investigation of meta data. 2. Representing a graph of all encrypted network traffic in the organization and using Graph Neural Network (GNN) algorithms. 3. Utilizing zero shot learning. The project shall conclude with a demonstration of the solution and its ability to identify malicious activity in encrypted traffic without decrypting it.
5. Human-Machine (AI) Interface Tools for Cybersecurity	Projects would focus on developing ways to include user interfaces and applications that incorporate human-factors engineering with machine-learning processes and front-end applications, in order to make it easier and for humans to use AI more effectively and securely, introducing an intermediate connection between the human and AI solution, reducing the difficulty and increasing the efficiency and cybersecurity of AI-related interactions. Potential approaches might focus on: 1. Analyst workflows and metrics to continuously evaluate usefulness of technologies (i.e., measuring how much screen time is spent on various types of software to determine pain points). 2. Non-survey-based tools that collect feedback from humans or evaluate what humans are doing day-to-day. 3. New human-AI teaming capabilities to support, inform, and enhance cybersecurity operations by deepening the understanding of AI's impact on human effectiveness. The project shall conclude with a technology demonstration of the findings.