Research Proposal Outline

Project Title

Active Cyber Defense for Airport Operation Technology (OT) networks

Significance/Contribution to the discipline/Research Problem

Airport OT networks like Baggage Handling Systems, Airfield Lighting, Airport Passenger Movement, Public Announcement Systems, etc, are disparate and air gapped. There is an increasing trend of cyber-attacks against airports, and OT networks are traditionally more focused on availability/reliability than security.

Research Question

Is it possible to have one cohesive active defense to protect against the increasing tide of cyber-attacks against Airport OT networks which would come under Critical National Infrastructure?

Aims and Objectives

Research and attempt to build an active defense strategy for airport OT networks addressing:

- OT vulnerability management
- Insider threats
- Cyber security awareness
- OT honeypots
- OT cyber security architecture

Key literature related to the project.

Below are a few of the literature being considered for the research. This is not a full list.

Piggin, R. and Buffey, I. (2016). Active Defence Using an Operational Technology Honeypot. 11th International Conference on System Safety and Cyber-Security (SSCS 2016). doi:10.1049/cp.2016.0860.

Smooam, C., Ontemporary, C. and Acedonian, M. (2019). MINISTRY OF DEFENCE REPUBLIC OF NORTH MACEDONIA. [online] 19. Available at: https://www.mod.gov.mk/storage/2020/02/37-Sovremena-Makedonska-Odbrana-en.pdf#page=11

Sundaram, A., Abdel-Khalik, H.S. and Ashy, O. (2020). A data analytical approach for assessing the efficacy of Operational Technology active defenses against insider threats. Progress in Nuclear Energy, 124, p.103339. doi:10.1016/j.pnucene.2020.103339.

Ellis, T., Balenson, D. and Locasto, M. (2022). Cyber Security Awareness Requirements for Operational Technology Systems. Critical Infrastructure Protection XV, pp.23–44. doi:10.1007/978-3-030-93511-5_2.

Lesser, M., Fellows, S. and Cox, O. (n.d.). Defending Operational Technology (OT) in Kinetic, Cyber, and Hybrid Warfare Darktrace Federal. [online] Available from: https://www.cisa.gov/uscert/sites/default/files/ICSJWG-Archive/QNL_JUN_2022/Defending%20OT%20in%20Kinetic%20Cyber%20and%20Hybrid%20Warfare_s508c.pdf

Methodology/Development strategy/Research Design.

Qualitative methodology

Ethical considerations and risk assessment (as part of your ethical approval application).

As an employee of an airport, the following will be ensured:

- Any participant I approach for an interview/survey will be informed and can opt-in.
- They would be informed of the intent of the research, what data will be collected, how it will be used and reported and how it will be collected.
- Ensure that no proprietary data is not used for research purposes.
- Provide assurances that the identity of any participant will be kept confidential.

Timeline of proposed activities.