Software Defined Networking (SDN) is inherently vulnerable to several network attacks, especially the Distributed Denial of Service (DDoS). Those attacks are recognized as a major jeopardy for network performance and generally lead to a network failure. Indeed, cyber attacks can easily overload the controller processing capacity and flood switches flow-tables.

Mitigation of cyber attacks can no longer be done with conventional techniques due to the emergence of new threats and processes used to launch those attacks. Today, the migration from defensive strategies based on “react after the occurrence of attacks” to offensive strategies based on “predicting the occurrence of attacks” is compulsory. Henceforth, AI-assisted security is an emerging paradigm in providing and preserving safe networks.

This Special Session provides a forum for broad and diverse audiences to discuss recent advances, challenges, and opportunities at the nexus of AI, networking, and cyber-security. The aim of this special session is to encourage research in areas such as design of attack-mitigation approaches, AI-assisted techniques of attack detection/classification/prevention and new ideas of self-healing networks.

Topics targeted by this special session include but are not limited to the following:

- Offensive Security paradigm
- AI-assisted security in SDN
- Prediction-based attack detection in SDN
- Classification-based attack detection in SDN
- Reinforcement Learning (QL)-based attack mitigation in SDN
- Online attack mitigationin SDN
- Network Self-healing approaches in SDN

Special Session Organizers:
Ali El Kamel, Manel Majdoub, and Habib Youssef
PRINCE Research Laboratory, ISITCom Hammam Sousse, University of Sousse.

Deadlines:
- Full Paper Submission: September 15, 2022
- Notification of Acceptance: September 21, 2022
- Camera Ready Submission: October 11, 2022

For any information, contact: sinconf@sinconf.org