Contribution ID: **49** Type: **Lightning Talks (5 minutes)**

Next Generation Security Operation Centres

Wednesday, 10 April 2024 16:25 (5 minutes)

NG-SOC considers the paradigm of interconnecting heterogeneous digital systems where traditional security controls are becoming increasingly inefficient due to the mosaic of the involved data, the plethora of diverse business services and the strong interdependencies between software components residing at interconnected infrastructures, allowing threats and security incidents to propagate between assets of these interconnected networks. At the user level, hand-held devices and mobile applications increase the system's attack surface.

Thus, the key-point to unlocking the enormous potential of the EU digital infrastructures serving millions of citizens, enterprises and society lies on their ability to remain cyber-secure. NG-SOC builds its concept on top of the actual cybersecurity needs of NIS Directive organisations. It has carefully identified the real-world cyber-security challenges that the consortium pilots currently face and through a systematic analysis has translated them to a set of desired attributes for the envisioned NG-SOC toolkit, including: early-stage detection and classification of attackers TTPs, identification of attacks caused by novel multi-faceted actors (both external and internal), actionable, relevant and accurate CTI sharing between organisations and devices, automated threat/incident detection, investigation and response (TDIR), automation and orchestration of incident response strategies and continuous learning (capacity building) and systematic raising and maintaining user awareness. NG-SOC aims to provide a holistic solution that exhibits the above attributes but most notably, addresses the challenges of the whole cybersecurity cycle.

Primary author: ANDREOU, Stephanos

Presenter: ANDREOU, Stephanos

Session Classification: Lightning Talks