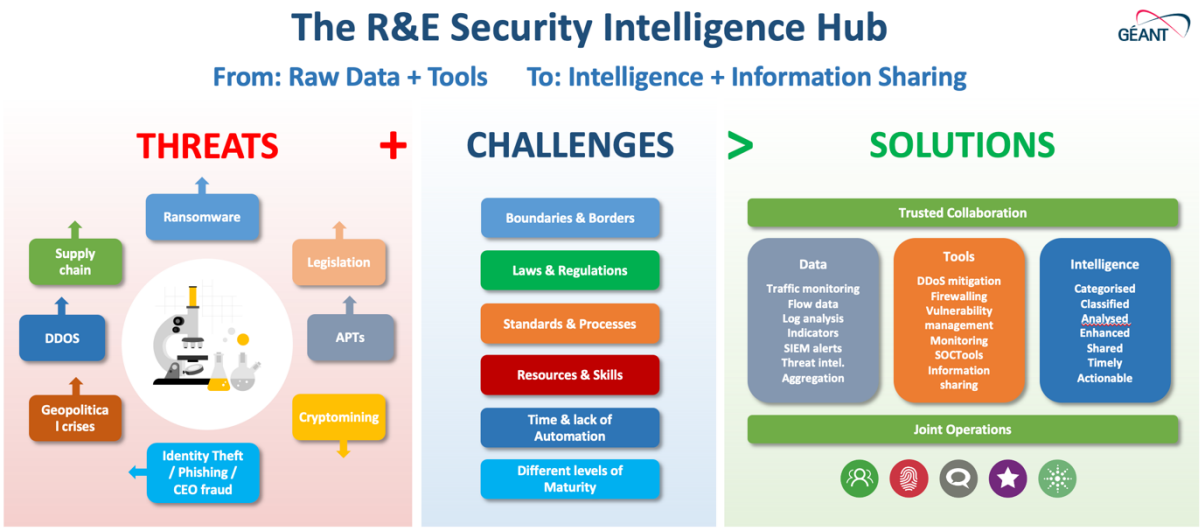
The Research and Education Security Intelligence Hub

Providing timely and actionable cyber threat intelligence by and for R&E

Intelligence providers have not traditionally focused on the research and education (R&E) sector for several reasons. The sector is likely seen to be not as profitable as others and sector-specific data is hard to come by; the limited available intelligence is unaffordable for most.

We want to change that, from within. Not to make money, but to save it – learning and collaborating, sharing operational capabilities and resources, building on communities – to create and share timely and actionable cyber threat intelligence (CTI) by and for R&E.

The Research and Education Security Intelligence Hub is a virtual organisation that seeks to create, collect, analyse, classify and share actionable security intelligence for research and education. The Hub is intended to counter specific cyber threats and challenges with solutions centred around trusted collaboration and joint operations; transforming raw data, with the help of specialised tools and analysts, into intelligence, that can be shared and acted on for the greater benefit of all participants.



The Hub provides a platform for security experts to create, collate, verify and share a range of threat intelligence as well as gain experience in utilising that intelligence effectively to protect our networks and systems. This intelligence and the resulting actions will give the community an edge over threat actors and attackers, facilitating the creation of a safe and secure environment for all R&E network users.

This presentation will outline the business model for the Hub centred around the value that the Hub delivers. Thereafter our current implementation journey will be explored, including:

- Threat intelligence sharing between RENs and NRENs – PoC experiences.
- Infrastructure and CTI tooling considerations and evaluation.
- Integrations and correlations – how we action threat intelligence and correlate with common data sources to create alerts, etc.

- Communication channels – how do we timeously share and communicate CTI?
- Information sharing agreements (necessary for distributing sensitive information).
- Not re-inventing the wheel – what can we learn from similar initiatives such as ISACs.

Finally, this presentation will conclude with a call to collaborate on the next steps in our journey to bring the Hub to maturity, inviting questions and discussion from the audience as feedback to guide our course and maximise benefit for all constituents.

Thank you for your consideration!