RESTENA open-source Security Operation Centre: protecting what matters

World events and the rise of cyber threats to global critical infrastructure, combined with the increasing awareness and growing number of security-related incidents are stimulating the demand for enhanced cybersecurity measures. The increasing complexity of R&E networks and product sets require more specialist skills. In response, several NRENs around the globe and connected institutions have coupled their established Network Operation Centre (NOC) with a Security Operation Centre (SOC). CONNECT met with Cynthia Wagner, Chief Information Security Officer for Restena, the Luxembourgish NREN, to talk about their requirements, plans and processes to build a SOC.

Interview by: Rosanna Norman, GÉANT

Cynthia, thank you so much for taking the time to talk to us. Can you share with our readers the steps that Restena has taken to create the SOC?

The very first step was observational: engaging in discussions with information security managers from major research and education institutions in Luxembourg and assessing the current situation across the entire community. These efforts clearly highlighted the absence and the need for a SOC.

Next, we investigated how to implement it, focusing on requirement analysis: needs and costs. Consistent with our internal culture, one requirement was clear from the start: we needed an open-source solution. We concluded that initiating an EU project would be the best approach as it aligns perfectly with our open-source strategy. We explored available funding options and successfully secured one! We then wrote and submitted the Enhancing Cybersecurity Services for the Luxembourgish Research and Education community (LuCySe4RE) project to the European Union's Digital Europe programme (DIGITAL).

With the LuCySe4RE project accepted and validated by the Restena board, we pooled our internal resources to take up the challenge. Finding these resources internally was easy due to the high motivation for this new service. We assembled a multidisciplinary team, including engineers from various internal services, and kicked off the project in September 2023.

With the team ready for the challenge, we then had to choose the right technologies, start implementing the technical infrastructure and onboard a few research and education institutions in Luxembourg. The project was immediately accepted for testing by our participants.

What technologies and tools will you be leveraging to build this new facility?

From the outset, it was clear that we would rely as much as possible on open-source technologies, and nothing could make us reconsider that decision. After thorough investigations, we identified a variety of components: Fluentbit, Logstash, OpenSearch, Suricata and the MISP platform, among others. We are particularly proud to use the MISP platform, developed in Luxembourg by our partner, the Computer Incident Response Center Luxembourg (CIRCL) of the Luxembourg House of Cybersecurity. MISP is not the only tool from our partners that we utilised in this project. We also employed the GÉANT **Security Baseline** to assess the maturity levels of the institutions participating in the project.

What challenges did you encounter during the implementation process?

Even though the implementation process is still ongoing and new challenges undoubtedly await us, one of the initial major obstacles was the sheer volume of data transmitted by the partnering institutions. This data already amounts to many gigabytes, despite not all institutions having onboarded yet!

Another significant challenge arose when we decided to rethink our initial infrastructure setup, switching from Elastic to OpenSearch. This decision was crucial for cost reduction and project simplification.

Will you monitor your network and your connected institutions, do you intend to measure security maturity levels?

Restena has been operating a NOC for many years monitoring all connected infrastructures. The future SOC and NOC will collaborate, as the data collected is valuable to both. In addition, the SOC will work closely with the Restena Computer Security Incident Response Team (CSIRT) to manage identified incidents, thus enabling advanced monitoring for our connected institutions.

Before implementing the SOC, we used the GÉANT Security Baseline to establish the current state of security maturity within Restena and the SOC-Project participants. This assessment will be repeated at the conclusion of LuCySe4RE, scheduled for August 2026. By doing so, we will be able to measure the evolution and overall impact of the LuCySe4RE project on Restena and the participating institutions.

How will the SOC handle customer-facing interactions out of hours? Will you outsource?

One of the first decisions was to operate the SOC only during office hours. Among our community members, there is limited availability to handle security alerts on 24/7. However, we are now exploring the possibility to include a CSIRT on-call duty, for internal purposes in the future. This initiative might inspire others to follow suit.

Which recommendations would you give to other NRENs who are planning to embark on a similar journey?

We have a robust and well-connected R&E network here in Luxembourg, with easy access to our institutions. Understanding their requirements is crucial. Once you've identified these needs, I highly recommend embarking on this journey. It is truly worthwhile! All you need is a dynamic and a motivated team, and thanks to the vibrant open-source community it's possible to access a variety of efficient open-source tools.

Restena is ready to offer assistance to any NREN looking to get started!

restena
LuCySe4RE
Enhancing Cybersecurity Services for the Luxembourgish Research and Education community
Co-funded by the European Union

Picture
The team of the LuCySe4Re

About Cynthia

Cynthia Wagner (fourth from left in the first row in the above photo) is the Chief Information Security Officer and Security Manager at the Restena Foundation, the national research and education network in Luxembourg. Previously, Cynthia was managing the Restena-Computer Security Incident Response Team. She graduated with distinction from the University of Luxembourg with a PhD in computer science, where she studied the effects of various data mining approaches on flow measurements for improving security. She is currently also an active member of different working groups at GÉANT. At a national level, she is a member of various advisory boards and the co-founder of Restena's CyberDay.lu and the Data Privacy Day conference. Cynthia is actively involved in teaching and in her spare time, she loves gardening and trying new recipes in her kitchen (whether she is successful or not).