Introduction

Background & core activity/activities of the organisation.
Interlan IX started in 2006 as a interconnection of a few small networks in Bucharest. Over the time has grown to become de largest IX in Romania, connecting almost all ISP in Romania and Moldova. We also have interconnection with most of the important content providers.
We have POPs in major cities in Romania and one in Frankfurt.

Size and location(s) of your organisation.
Interlan IX HQ is located in Bucharest. We have 5 permanent employees, 7 board members that are working pro-bono and we are closely collaborating with a company for assuring technical operations.

Department(s) that will be involved in the project.
We will involve tech department and probably one person from administrative department. The board members will be continuously informed about the project.

Indicative time: 1 minute

Connections to the Call

Why/how is this Call relevant/important to your organisation(*) & how do you see your role in the project?

Anomalies detection is part of day to day operation of an IX. It will help us better understand the traffic flow, the possible issues and how to handle them. Also it will help ensuring a higher security level around the internet.

Past activities or experiences with the Call topic?

We are actively monitoring the traffic flows and levels in the IX. On personal plan, I owned an small ISP in Bucharest and did a lot of research on improving traffic flows, for a better end-user experience.

Indicative time: 2 minutes

(*) See for reference the starting document and visualisation for details about the project concept on Indico.

Specific interest & expertise

What are your direct interest areas in the SHIELD project?
Improving the traffic flows, detecting and/or eliminating unwanted/unusual traffic.

What technical expertise do you have within the organisation to address the challenges in the Call and in the SHIELD description (*see also starting document and visualisation for details about the project concept*)?
I was a lead network admin for a small ISP that grow in more than 15 years from using a 2Mbps uplink to multiple 10Gbps uplinks. One of my “passion” was to ensure that what mattered for the end user was working flowless.
In the last years I worked in parallel on a network monitoring solution that is based on events, anomaly detection and corelation being a big point in the process.

Could you also briefly describe the days analytics team you have in your organisation?
Usually we are monitoring traffic levels and reactively the problems that occurs.

Indicative time: 2 minutes

Envisioned use of SHIELD project results

Could you characterize the data (kind, frequency, bandwidth) you have, and what you do with that data ?
We have an average of 400Gbps of traffic. For the moment we are using specialized software to monitor traffic levels between different ASNs and ports.

Could you briefly give a few examples of potential attack vectors that have a data footprint?
From our point of view biggest attack are floods of data. Other things that we are monitoring are fluctuation in IP addressees counts received from peers and movement of IP blocks between peers.

Where/ how could the project results be embedded in your organisation ? (*organisational, hierarchical*)
The project would be very helpful in monitoring actual and preventing future issues. It will give us a better overview on what is flowing through out network, lowering the work done for identifying and corelating sources of problems.

What would be your envisioned integration path for the project outcomes inside your production system ?

Indicative time: 4 minutes

Project outcomes

What would be the optimal outcome of the project for your organisation?
A better understanding on what data we need to extract and how to use the data we have in order to make a more stable IX and prevent issues and abuses on network.

To which network(s)/audiences do you have access to present project outcomes?
Major ISP in Romania and Moldova, public networks, law enforcement agencies and other players from different domains (energy, banks, stock exchanges).

Indicative time: 1 minute