Master Thesis – Endpoint Detection and Response in Mobile Networks

Background
Ericsson is investigating the possibility to deploy Endpoint Detection and Response (EDR) capability in embedded mobile network equipment to detect and respond to intrusions in the nodes. The EDR system consists of detection functionality deployed on the end hosts and an infrastructure for managing both the configuration and the alerts generated by the EDR SW. Detection capability can be both local and centralized for correlation with events from other nodes in the network. Implementing EDR functionality in embedded nodes in mobile networks provide some unique challenges when it comes to limited resources in the node (e.g. storage and computational power) and scalability in networks with tens of thousands of nodes.

Thesis Description
The following steps are envisioned as part of the thesis work:

- Investigate and compare techniques for implementing an EDR system on embedded nodes regarding detection capability, footprint on the node and scalability in large networks.
- Propose a deployment model and test the system behavior (e.g., detection rate, node overhead and network load) using simulations or real test equipment.
- Analyze the results of the tests and evaluate the proposed model.

The thesis will be concluded with a result presentation for the Ericsson team.

Qualifications
This project aims at students in electrical engineering, computer science, computer engineering or similar. Background of Linux, IT security and network communication is preferred.

Extent
1-2 students, 30hp each

Location
Ericsson AB Mjärdevi, Linköping

Preferred Starting Date
Spring 2022

Keywords
Mobile Telecommunication, Security, Embedded, Linux

Contact Persons
Joakim Aronius
+46 724 650 809
joakim.aronius@ericsson.com