ABSTRACT:

NETWORK INCIDENT HANDLING

Tiszai Tamás, tiszai@sztaki.hu
Tóth Beatrix, btoth@sztaki.hu
Becz Tamás, becz@sztaki.hu
Pásztor Szilárd, don@sztaki.hu
Rigó Ernő, rigo@sztaki.hu
MTA SZTAKI

The aim of this tutorial is to give an overview on the possibilities of securing small and medium sized IP-based networks with Internet access, on the physical and management levels, also taking care of the handling of incidents uncloaked by utilized defense and intrusion detection systems. Under the course of the presentation we will also talk about collection and analysis methods of information and evidence left behind by occurred incidents.