

SOC4CI

Digital Infrastructure

SOC4CI



Detecting and responding to the undetectable

SOC4CI develops a security operations centre for critical infrastructures. It provides a customized detection and response service against Advanced Persistent Threats (APT).

In December 2016, an electric power substation in Kiev was cut off from the main power grid for hours, and 20% of the city's population was left without electricity when temperatures were far below zero.

SOC4CI integrates a wide range of public and private security information sources, and uses a real-time stream processing framework for event correlation and

anomaly detection. The advanced technical solution is combined with an expert incident response team for providing a turnkey managed security monitoring service.

SOC4CI allows utilities to make the most out of their security investment, while at the same time it offers real-time situational awareness.



Competitive Advantages

- Integration of multiple sources of security information used in a critical infrastructure into a single state-of-the-art security incident and event monitoring system (SIEM)
- Prompt detection through real-time stream processing, combined with off-line machine learning
- Turnkey managed detection and response service based on expert incident response team
- Ease of use and low cost of ownership



Target Markets

- Critical infrastructure including energy sector
- Mid-size (500-10K employees) regional companies
- European market, Nordics as lead



Status/Traction

- Service design project run
- Several pilots and lead customer trials



Road Map

2018

- Support for vehicle applications
- Support for BYOD
- Distributed SOC architecture for improved compliance
- Reseller partner business model and support

2019

- Scale-up



Connect



György Dán
SOC4CI Activity Leader
e: gyuri@kth.se
t: + 46 8 790 4253



Location

SOC4CI

c/o KTH/E

Osquldas väg 10

10044

Stockholm

Sweden

Partners:

Bittium, Budapest University of Technology and Economics, F-Secure, KTH Royal Institute of Technology and SafeMove

SOC4CI

SOC4CI is an Innovation Activity proudly supported by EIT Digital



Digital

eitdigital.eu

f y i n t @EIT_Digital

Driving Europe's Digital Transformation