Swedish IT Incident Centre (SITIC) gives market neutral IT security to the public and private sector

oskar.bergquist@sitic.se
Structure

Working groups

CERT/CSIRT
Politics & Outreach
Software/system development
Operations

24/7 duty officer for government & CERTs

CSIRT officers (+ administrative personnel)
Service levels

Regular CERT activities

Technology watch, short and long term (vulnerabilities and other threats)
Handling of abuse (phishing, defacements)
Attack mitigation (digital forensics, DDoS dampening)

Extra services

24/7 incident handling
Homebrewed tools for intrusion detection, technology watch, web security and more
Expert knowledge sharing and support
Tools - MolluskNG

An extensible, customizable web fetcher

Finds new links in HTML pages, RSS feeds, and Mailman pages

Export: HTML mail, and RSS feeds
Tools - Megatron

A system that collects and processes info about bad hosts on the Internet

In production since Christmas 2009

Typical statistics for a week:

>10 million log lines processed
>50 000 log records saved in db
~50 abuse email sent (no ISPs or universities)
New home 2011

From

The Swedish Post and Telecom Agency (PTS)
Telco regulator

To

The Swedish Civil Contingencies Agency (MSB)
”Former” SEMA