VALTIOVARAINMINISTERIÖ

Valtionhallinnon häiriötilanteiden hallinta – miten VIRT-toimintaa kehitetään?

10.12.2015 VAHTI-päivä – Kirsi Janhunen

Mihin häiriötilanteiden hallinta perustuu

- Hyvään tilannekuvaan
- Sujuvaan viestintään
- Selkeisiin rooleihin ja valtuuksiin
- Sujuviin ja tarvittaessa tilanteeseen mukautuviin prosesseihin
- Toimivaan päätöksentekoon

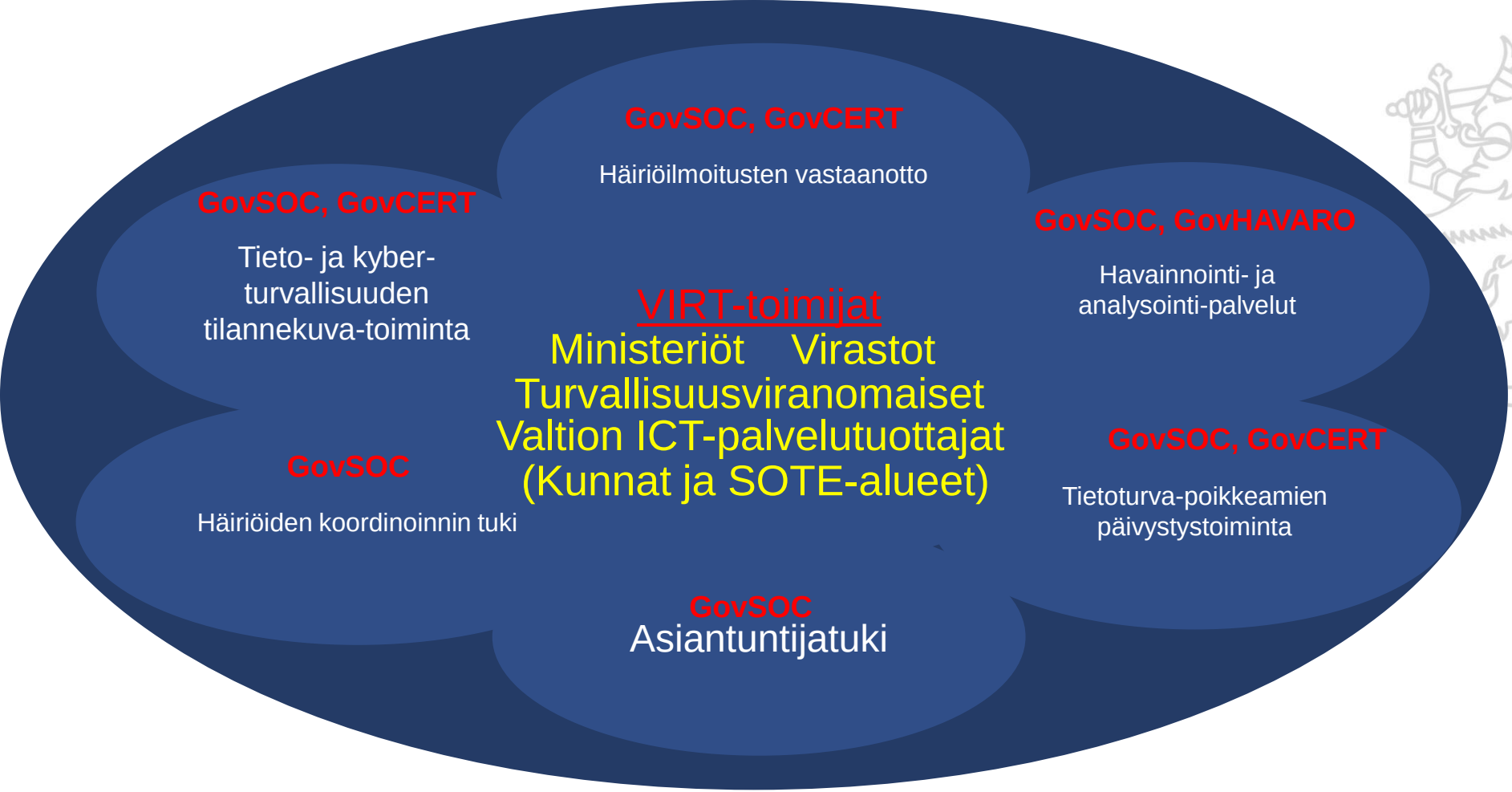
➢ Näitäkin asioita kehitetään VIRT-toiminnassa.

Mitä on VIRT-toiminta?

- Julkisen hallinnon organisaatioiden poikkihallinnollista operatiivisen tason yhteistoimintaa, joilla varaudutaan vakaviin ja laajavaikutteisiin tietoturvapoikkeamatilanteisiin.
- Toiminnassa suunnitellaan ja harjoitellaan toimimista erilaisissa tietoturvapoikkeamatilanteissa.

VIRT-toimintaa on käynnistetty vaiheittain

- Toiminta käynnistettiin syksyllä SecICT-hankkeen pilottina 2014 pienellä, eri hallinnonalat kattavalla kokoonpanolla. Mukana myös muutama pilottivirasto.
- VIRT-toiminnan suunnitteluun liittyi GovSOC-konseptin suunnittelu
  - Nyt konsepti on valmis. Vuoden 2016 aikana mukaan kutsutaan kaikki virastot.
  - Suunnitelmissa laajantaa toimintaa myöhemmin kuntiin ja SOTE-alueisiin.


GovSOC, GovCERT
Häiriöilmoitusten vastaanotto
GovSOC, GovCERT
Tieto- ja kyber-turvallisuuden tilannekuva-toiminta
GovSOC, GovHAVARO
Havainnointi- ja analysointi-palvelut
VIRT-toimijat
Ministeriöt Virastot
Turvallisuusviranomaiset
Valtion ICT-palvelutuottajat
(Kunnat ja SOTE-alueet)
GovSOC
Häiriöiden koordinoinnin tuki
GovSOC, GovCERT
Tietoturva-poikkeamien päivystystoiminta
GovSOC
Asiantuntijatuki

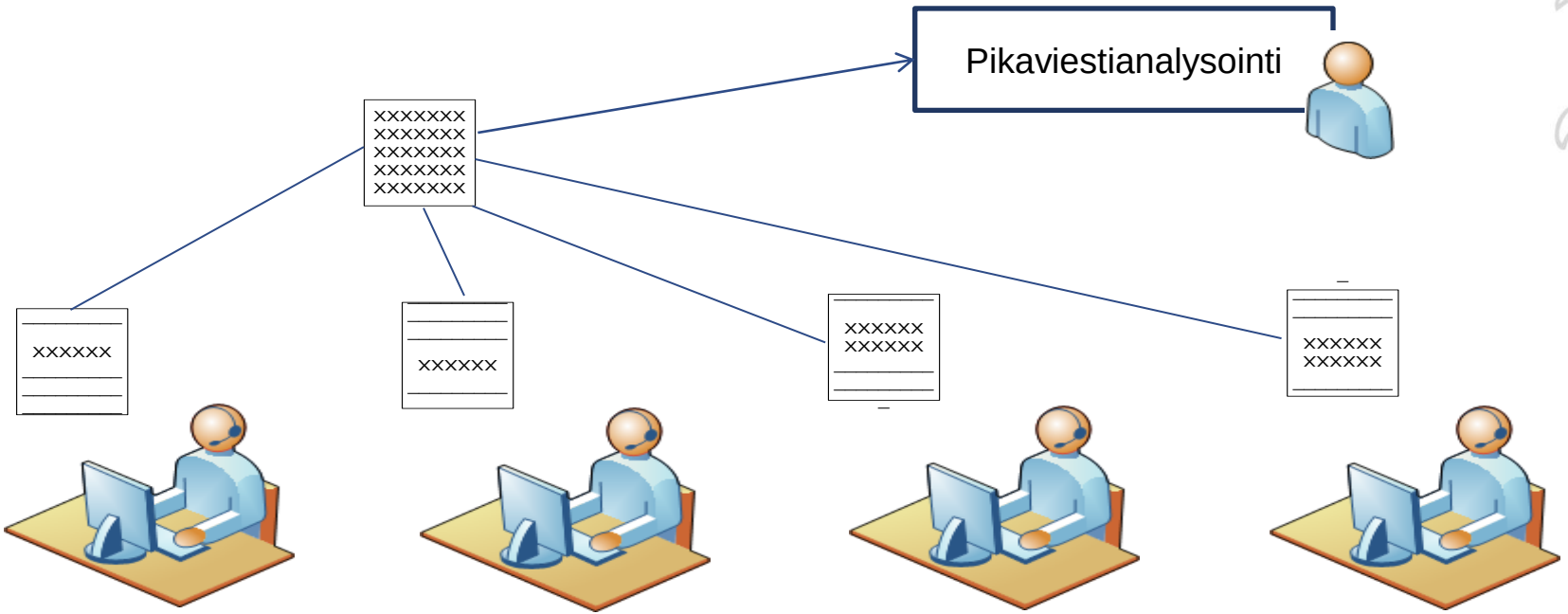
Mitä VIRT-toiminnassa tehdään

- Suunnitellaan ja harjoitellaan yhteistoimintaa laajavaikutteisiin ICT-poikkeamatilanteisiin
- Suunnitellaan yhteistyössä, millaisia palveluja tarvitaan toiminnan tueksi
- Jaetaan tietoa
- Opitaan tapahtuneista
- Verkostoidutaan ja saadaan ammatillista ja henkistä tukea

SecICT-hankkeen tuloksia tähän mennessä

- Viranomaisten yhteistyöverkoston perustaminen (VIRT)
- Häiriöiden hallinnan tuen kehittäminen (mm. päivystystoiminta ja haavoittuvuuskoordinointi)
- Havainnointikyvyn parantaminen
- Kustannustehokas kokonaisuuden hallinnan konsepti luotu (GovSOC)

Pikaviesti


Pikaviestianalysointi
xxxxxxx
xxxxxxx
xxxxxxx
xxxxxxx
xxxxxxx
xxxxxx
xxxxxx
xxxxxx
xxxxxx
xxxxxx
xxxxxx

”ITSM, CMDB, GRC” osana tietoturvallisuuden hallintaa

- Valtoriin kootaan keskeiset toimialariippumattomat ICT-palvelut, samalla sinne muodostuu keskeistä ICT-ympäristötietoa
- CMDB-tietoa voidaan käyttää järjestelmien kriittisyyden, riippuvuuksien ja tietoturvallisuuden tilannekuvan muodostamiseen
- Valmisteilla demo, jossa luodaan tilannekuva YTS-kriittisen järjestelmäympäristön vakavasta tietoturvapoikkeamasta.
- GRC = Governance, Risk and Compliance

Miten VIRT-toimintaa kehitetään jatkossa?

- Toiminta virallistetaan
- Laajennetaan toimintaa koskemaan koko julkista hallintoa
- Muodostetaan VIRT-alaryhmiä
- Valmistellaan tarvittavia sopimuksia ja suunnitellaan yhteistoimintaa
- Kehitetään toimintaa harjoitusten ja toiminnan kautta
- Varmistetaan, että säädökset ja normit tukevat poikkihallinnollista yhteistoimintaa häiriötilanteissa
  - ➢ VIRT-toiminta muodostuu jäsentensä näköiseksi