Incident Response in multiple Service-User-Relation layers and threat intel sharing in challenging environments

Sven GABRIEL, David CROOKS

EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777536.

Introduction

- Other examples of “operational security nightmares.”
- What went wrong.
- What the impact was.
- How to address the issue and mitigate the impact.
- Threat intel sharing in challenging environments.

Incident Response in different Environments

Incident Response, Traceability

SECURITY TRACEABILITY AND LOGGING POLICY

The minimum level of traceability for use of the IT Infrastructure is to be able to identify the source of all actions (executables, file transfers, pilot jobs, portal jobs, virtual machine management, image management, etc.) and the individual who initiated them.

Incident Response, Simple environment

- Organisation owns hardware.
- Systems managed by the organisation.(including: What is stored, who has access to the personal data -for which purpose, retention times, etc)
- Organisations security team has full access to relevant logs

Challenging Environments

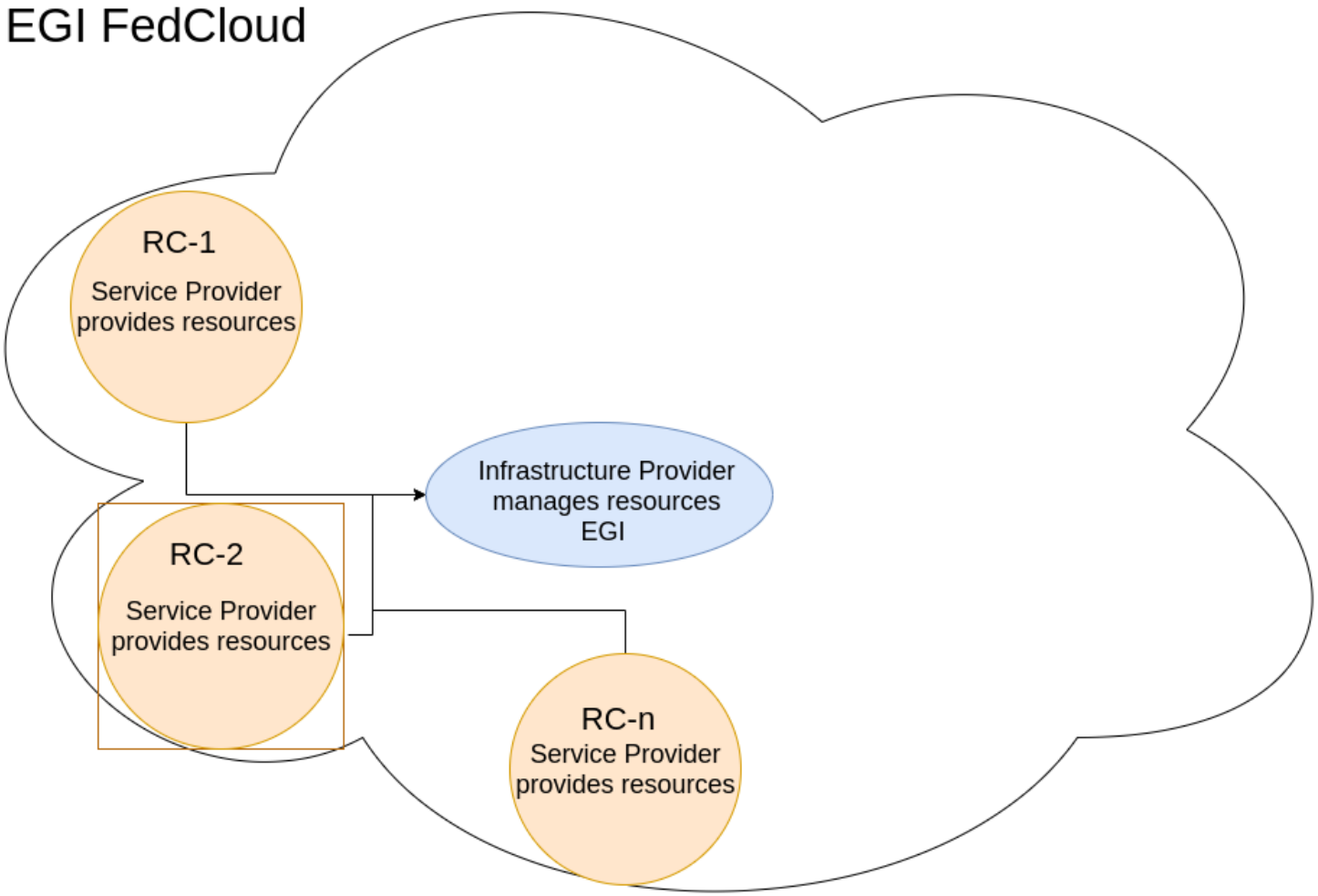
Incident Response, Questions/Requirements

- Responsibility, liability. Who needs to react/work on an incident?
- **Communications** to responsible CSIRT.
- Who has legitimate access to which data?
- To understand an incident access to logs of affected systems needed.
- Chances of incident resolution depend on strict adherence to policies/procedures.
- Complexity of IR depends on environment, existing agreements.

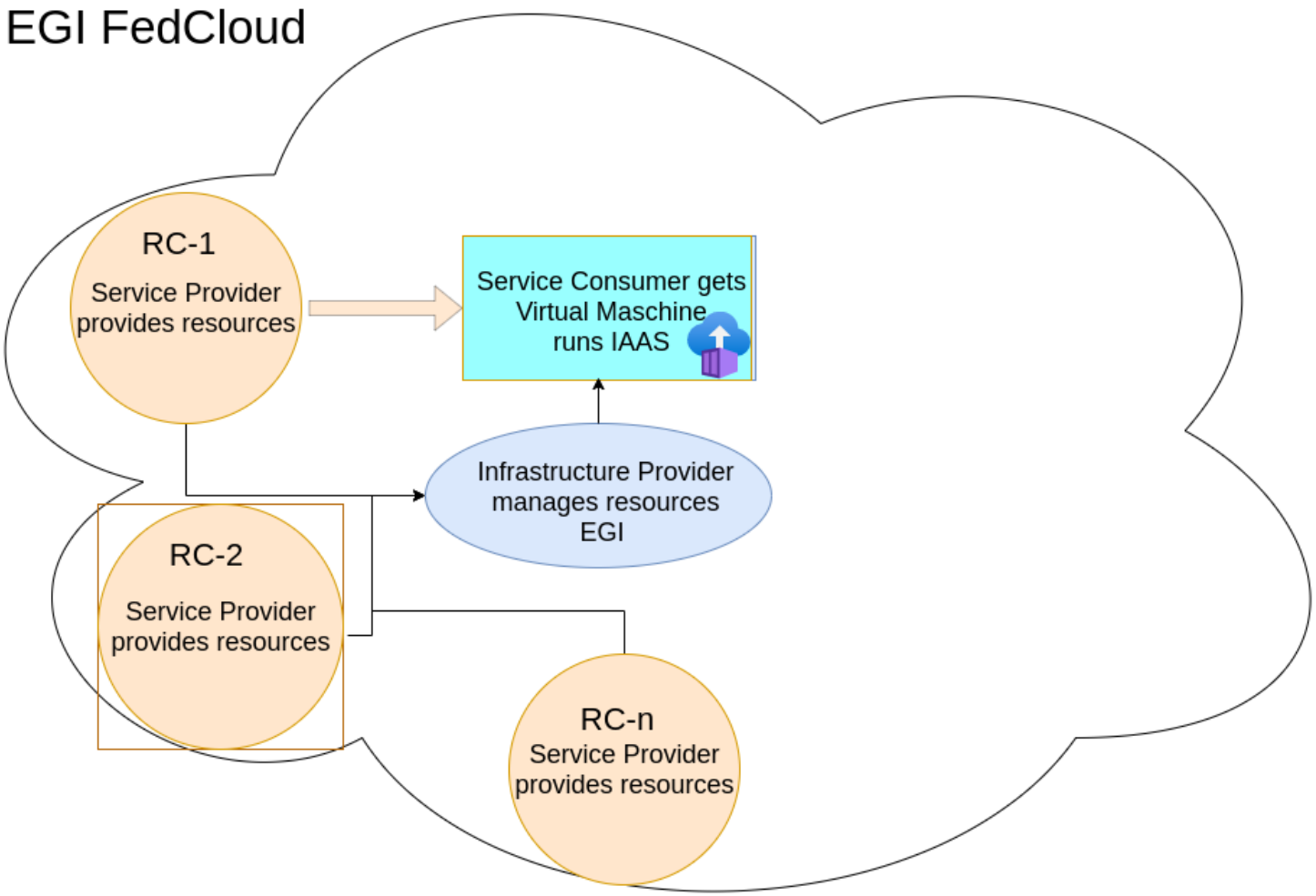
Service Provider/Consumer layers I

- Simple case: VM on Cloud Provider
- Company owns/manages the infrastructure, is the Service Provider.
- Service Consumer (User)uses VM to process personal data. Is the data controller.
- From GDPR perspective: Service (VM) Provider is Data Processor.
- Service (VM) Provider collects/processes accounting data of the Service Consumer (User). Is the data controller of this data.

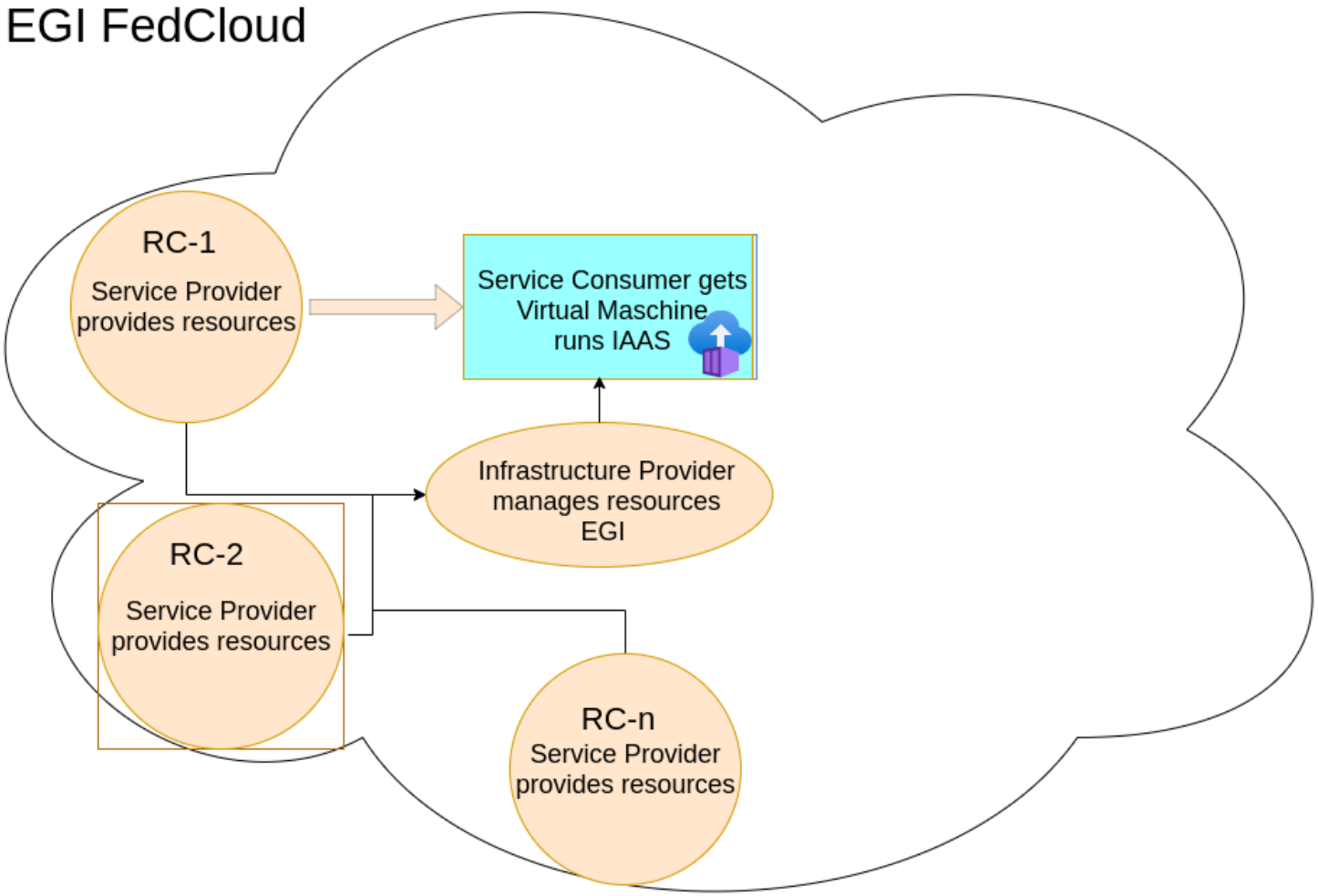
Multiple Service-User relations



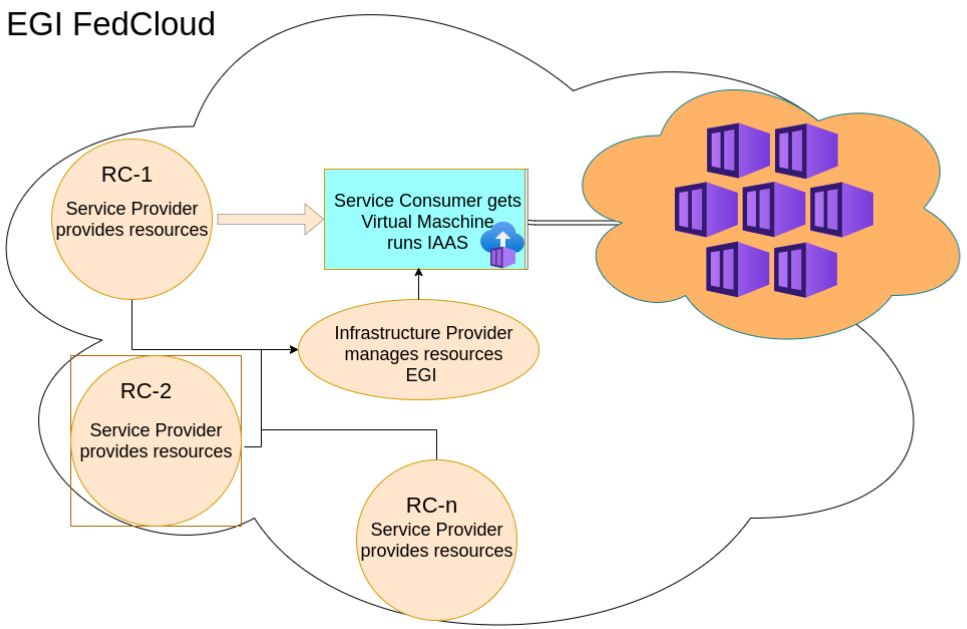
Multiple Service-User relations



Multiple Service-User relations



Multiple Service-User relations



Service Provider/Consumer layers II

- Log data locations.
  - Log data at RC-1.
  - RC OLA, RC is data controller
  - Log data in a Container which is started in a VM at RC-1
  - Similar statement in VO-SLA? In particular who is responsible for Incident Resolution.
- Communications/Reporting
  - RC OLA *Incidents must be immediately reported to the EGI CSIRT according to the SEC0113 procedure.*
  - Similar statement missing in VO-SLA

CSIRT Minimum Recommendations

Prepare for incident response

The relevant Agreements (SLAs, OLAs) between **all** involved parties need to cover:

- All used services need to have sufficient logging functionality to allow for traceability, as described for example in Security traceabillity and logging policy
- Who/Which security team is responsible for security incident response? This team needs a sufficiently robust mandate to get access to all relevant data.
- Communication infrastructure: where to report security incidents, security contact information for all involved entities available to the security team.
- Escalation procedure and decision making.

Threat Intel sharing

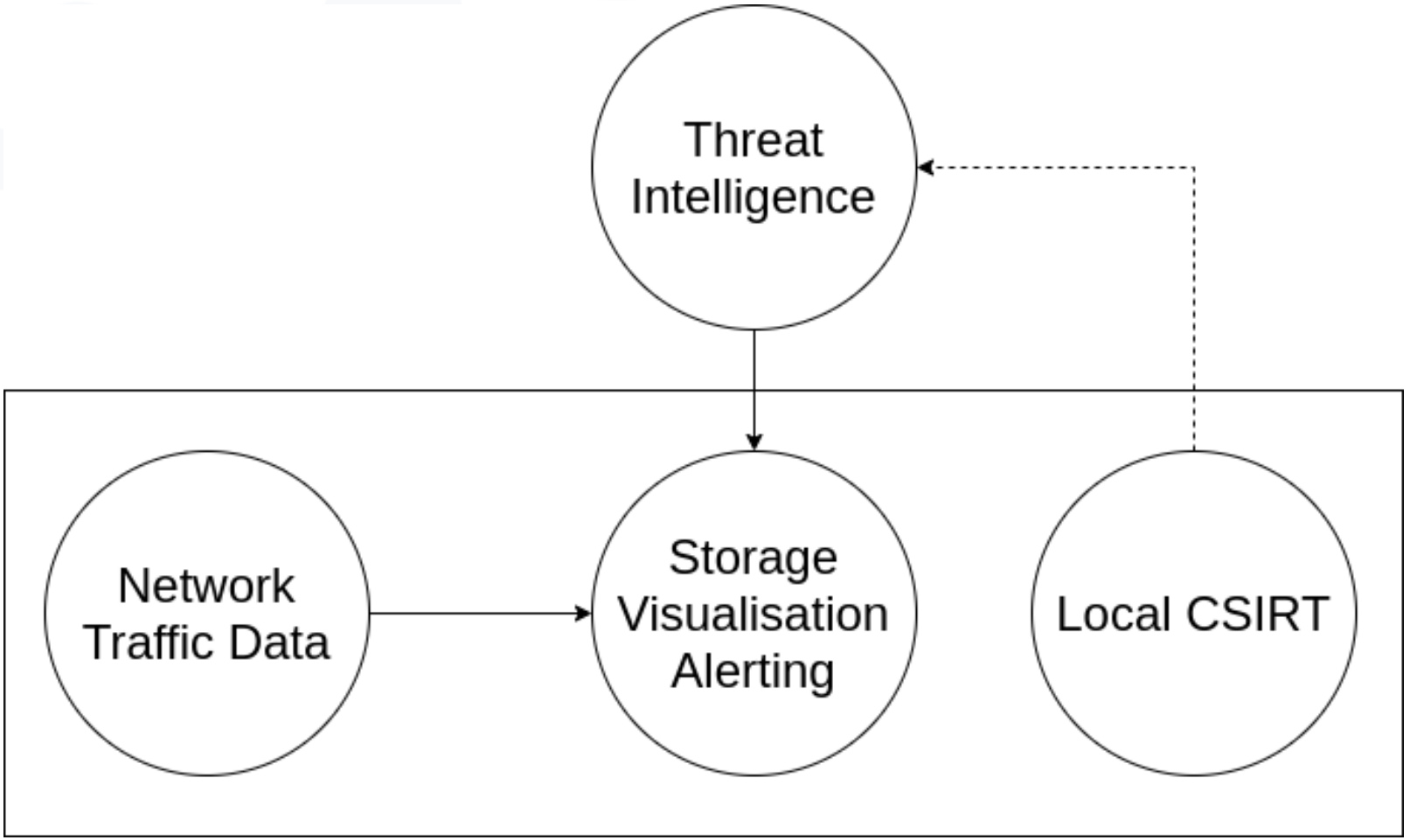
Threat Intel, some context

- Threat Intel sharing is about sharing information acquired during incident response with other security teams.
- Threat intel or *Indicators of Compromise* (IoCs) can be used to check if an organisation is affected/victim of a known attack.
- External threat intel is available. Quality of info varies.
- Specific threat intel for our environment would be very valuable.
- This (huge amount) of information is typically processed in a Security Operations Center (SOC)

Security Operations Centres

- Need to integrate
  - Threat Intelligence
  - Network traffic data
  - Storage, visualisation and alerting
- **Security Operations Centre (SOC)**
- WLCG SOC working group has been designing reference designs for several years
  - Learning from more complex production CERN SOC
  - Much broader than WLCG in membership

SOC


Threat Intelligence
Network Traffic Data
Storage Visualisation Alerting
Local CSIRT

WLCG Strategy

- Deploy SOCs at Tier1 sites
  - Biggest immediate impact
  - Support national communities
  - Typically close links with NRENs
- Activity at several Tier1 sites including existing CERN SOC, in production for several years
- Source of threat intelligence for research and education sector hosted at CERN

- Many EGI sites are part of WLCG work
- More broadly particularly important to work with cloud providers
- Network monitoring a vital tool in securing these resources
  - Join the working group!
  - Aim to have one global effort for research and education sector in deploying these type of SOCs

SOC working group contacts

- Website and documentation
  - wlcg-soc-wg.web.cern.ch
  - wlcg-soc-wg-doc.web.cern.ch
- Egroup
  - wlcg-soc-wg@cern.ch
- David Crooks (david.crooks at cern.ch)
- Liviu Valsan (liviu.valsan at cern.ch)
- Access to CERN MISP
  - wlcg-security-officer at cern.ch

Any questions?