EUDAT/EGI-CSIRT F2F Jan. 2018

EGI-CSIRT

EOSC-Hub

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142

EUDAT/EGI-CSIRT F2F Jan. 2018

EGI-CSIRT

EOSC-Hub

Intro/Logistics etc

Intro

- Logistics (Vincent)
- Agenda/Intro
- Monday Afternoon . . . DaveK/Urpo

Agenda

Agenda

Agenda:

- Agree on Agenda (see indico)
- Minute Takers ?
- Summary last F2F (brief)

Nov 2017 Meeting

Summary F2F Nov 2017 Helsinki (CSC)

Summary Nov 2017 Meeting

- EGI-CSIRT/EUDAT/EOSC and all the rest
- Result: Yes, we want to integrate.
- Rough ideas presented at DI4R

EUDAT EGI-CSIRT Coordination Integration

- Common F2F meeting held in Helsinki (Nov 2017)
- Policy
  - Full cross-review, alignment, and create road-map.
  - AUP alignment & GDPR are early priorities.
- Procedures
  - Alignment of the Incident Response Procedures.
  - Ensure maintained contact details to all sites are available.
- Incident Response
  - EUDAT Security observing member in EGI-CSIRTs IRTF
- Incident Prevention
  - Monitoring EGI and EUDAT teams to review options for collaboration.
  - Vulnerability: SVG will investigate possible collaborations.

Agenda

Agenda:

- Tuesday:
  - IRTF Debriefings
  - Trainings/Certification Curriculum
  - SSC Dirac
  - Lunch
  - SVG Business
  - Goals and next steps towards EGI-CSIRT/EUDAT integration

Training/Certification

Security Trainings

EOSC WP 11.4.10 (google sheet)

- 3 Foundation Trainings in 2018 (incl. exams)
- First event Taipei 20. March 2018
- Exam/Certification in testing
- 1full day, tentative schedule . . . next slide

Schedule

- 09:00 09:15 Introduction
- 09:15 - 10:30 The Threat Landscape: Introducing terms in context of ENISAs Threat Landscape Underground economy
- 10:30 11:00 Coffee
- 11:00 - 11:45 Malware Techniques
- 11:45 - 12:30 Demonstration of typical attacks on FedCLoud Virtual Machines
- 12:30 14:00 Lunch
- 14:00 15:30 Discussion and Hands-on of operational security for Cloud User Communities session 1
- 15:30 16:00 Coffee
- 16:00 - 17:20 Discussion and Hands-on session 2
- 17:20 Wrap up/conclusions

Material / HandsOns

- Slide Deck from TI, licence currently under discussion (CC)
- based on Enisa Thread Landscape
- Interplays, get the people talking, may be difficult in Taipei :)

Enisa TL

Interplays

- Group Discussion: Threats, Ask them about Heartbleed and Shellshock. Ask them about the difference between traditional threats and cyber threats. For the rest of the module, we omit the term cyber and talk about threats only. Goal: Match the outcome of the Group Discussion with the ENISA Threat Landscape
- Malware Techniques: Develop Interplay with relevance for CloudAdmins, i.e. malware technique they have to deal with, automated attacks.
- Demonstration of typical attacks on FedCLoud Virtual Machines. **What to do here?**
- RolePlay Handle Incident, goal: understand the need for coordinated ir, how VO sec. teams could interface with IRTF?

What else? Policies

- VM Endorsement policy https://documents.egi.eu/document/2729
- https://wiki.egi.eu/wiki/Virtual_Machine_Image_Endorsement Enol, Vincenzo
- Roles: Endorsers, VM Operators (incl Policy requirements), like
- *you are responsible to fulfil/to ensure . . .*
- *If the VM image is endorsed then the instantiation may be considered to be trustworthy up to the point of contextualisation*

What else? VO roles

- VO-Box manager
- VO Security Contacts
- more ?

Who to train?

- Site Admins?
- Cloud Users
- ?

Branches

- IAAS Infrastructure Admin
- IAAS Incident Responder
- Managers

Levels

- Basis
- Advanced
- Expert

Minutes Mal

Decisions:

- Training will go with EGI certification and we will not involve at this step external CA
- We will start with two foundation training for EGI federation 2018 e.g. core services providers
- Single training+exam should take 1-2 days
- Exam would take 1-1.5h
- (Optional Leif+2 people will cost 5k in Europe - all included)
- We (EGI CSIRT) have potentially 8 people willing to deliver training (this was an assumption by Sven:)
- Security materials are getting out of date so maintenance is very important
- In the future investigate online foundation training as an option

Minutes Mal II

Short term goals:

- Decide on the structure of certification - levels, components of each level. - example http://fitsm.itemo.org/fitsm-training
- For each component (training with certification) should be provided scope statement and matching existing courses

Exam

Exam / Certification (Urpo)

Service Certification

Service Certification, Why

Problem:

- Users start from good VMs (**This remains to be confirmed**)
- To deploy a compute cluster in the cloud, orchestration is used. Ansible scripts used, credentials (ssh root) delegated to service, magically VM spawn up, cluster initialized. This needs to be a **trusted** service. (other example: GCE (Google Compute Engine), CLIC (Cluster in the Cloud) Linux-Journal-2017-11.pdf)
- Introduced issues:The attacker made use of an improperly secured NFS server which was open to the Internet. The NFS configuration resembled the following (located usually in /etc/exports):
  /localdata/home
  (rw,sync,no_subtree_check,no_root_squash)

Service Certification, Why

Problem:

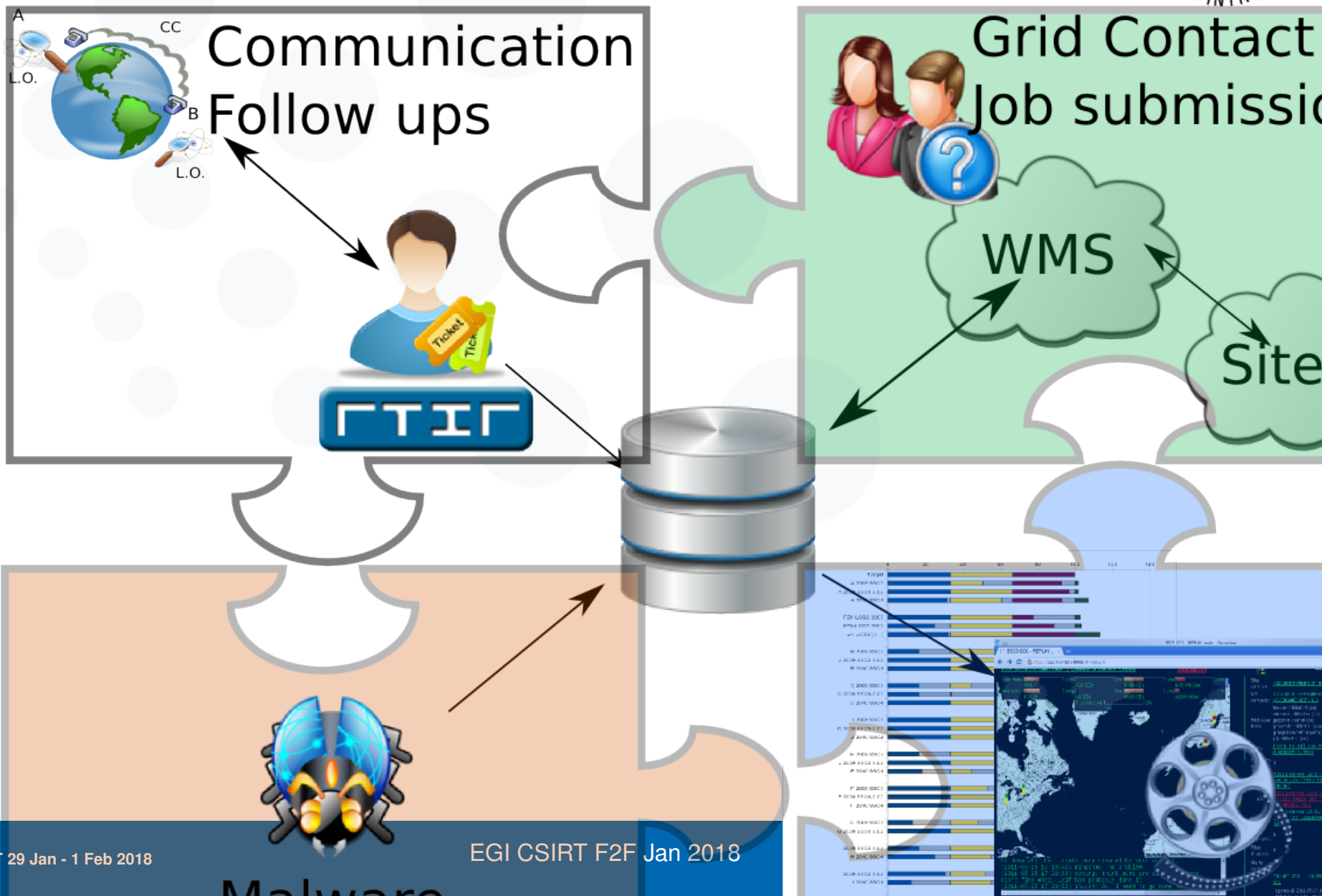
- Discusion how to make sure that for example ceetain Galaxy Servers in EGI can be trusted.
- Goal: Develop workplan for OMB. (Task is mainly Operations anyway)
- Complicating factor, new CTO.

SSC Dirac

Subsection 1

SSC DIRAC

DIRAC SSC


A
CC
L.O.
B
L.O.
Communication
Follow ups
Ticket
RTIR
Grid Contact
Job submissio
WMS
Site
Malware

DIRAC SSC

- Used WMS: DIRAC
- VO (LHCB), ready to go UI needed, accessible via ssh from few IPs, Use VO-Testbed for submitting/running jobs.
- VO-? EGI, ready to go UI needed, accessible via ssh from few IPs
- Communications RT-IR (”handle as normal incident?”)
- Build botnet, Malware controlled via cnc (to be connected to SSC-Monitor)
- Monitoring with icinga2? WN $\rightarrow$ Monitor
- (UIs to be connected to SSC-Monitor)
- Report: Template/skeleton has to be ready before the SSC starts.

DIRAC SSC Schedule

- Planning/Preparations start now.
- SSC Tentative Date Week: 29 (16h- 20th June), later would be summer break.
- Workpackages to be defined here :)
- Coordination challenge :) multiple groups involved, important to have the building blocks ready to be assembled by week 18.

DIRAC SSC Workpackages

- Preparations:
  - attacker id etc, checklist on SSC-8 wiki i
- SSC Tentative Date Week: 29 (16h- 20th June), later would be summer break.
- Workpackages to be defined here :)
- Coordination challenge :) multiple groups involved, important to have the building blocks ready to be assembled by week 18.

SSC Challenge-Infra

- LHCB (Christphe?)
- UI accessible via ssh with command set (scripted?) to submit jobs with defined payload.
- IR info for sites (how does dirac work, where to intercept job flows, contain incidents, stop jobs)
- IR Plan (coordinate with IRTF, and ?)

Stage-1 Communication Challenge

- Start of Challenge (SoC) - 2 weeks
- Use the foreseen communication infrastructure.
- Sites that fail to be handled by Operations.
- Sites that pass, can participate.

Stage-1 Communication Challenge

Purpose of this stage is to make sure that the automated communication channels to the RC security teams are working as expected. For targeted communications in larger campaigns we use a tool developed within our team that, based on the RC names queries the GOC-DB for the RC and NGI security contact information and opens a ticket in RT-IR to the RCs, CCing the NGI security contact. The RCs were asked to acknowledge the message within 24 hours by replying to the mail/ticket.

Stage-2 Infect sites

- Time constraints (max lifetime of jobs)
- may require multiple jobs per site, sites have to check their logs.
- SSC-Monitor needs logging for that i

Summary Stage-1 Communication Challenge

As a result we found that all RCs responded within the required time frame, the contact information in GOC-DB is up to date, and EGI CSIRTs communication tools are working as expected.