Organizing Operational Security in evolving distributed IT-Infrastructures

Sven Gabriel, Nikhef/EGI-CSIRT

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

Introduction

Introduction:

- Operational Security
- Evolving distributed Infrastructure
- Status IR tools development

Operational Security

Operational Security

- Incident Prevention (sec-mon, vulnerability handling)
- Incident Detection (reporting)
- Incident Response

All operations in these fields will affect the usability/availability/accessibility of the services. You can not do anything here without the mandate of the management / a policy framework.

Operational Security

Components

- Policies (Define the pitch)

Operational Security Policies

Policies, example http://aws.amazon.com/service-terms/
57.10 Acceptable Use; Safety-Critical Systems. Your use of the Lumberyard Materials must comply with the AWS Acceptable Use Policy. The Lumberyard Materials are not intended for use with life-critical or safety-critical systems, such as

. . .

aircraft or air traffic control, nuclear facilities, manned spacecraft

. . .

Operational Security, ?

Policies, example

. . . sure, . . . But, what if

Operational Security, ?

Policies, example

. . . sure, . . . But, what if

Operational Security, ?

Policies, example

. . . sure, . . . But, what if

Operational Security Policies

Policies, example http://aws.amazon.com/service-terms/

. . .

However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization. [1]

[1] lumberyard is a free, cross-platform, 3D game engine to create games

Operational Security Policies

Policies, EGI AUP

https://documents.egi.eu/public/ShowDocument?docid=74

7. Use of the Grid is at your own risk. There is no guarantee that the Grid will be available at any time or that it will suit any purpose.

. . .

9. The access-granting bodies and Resource Providers are entitled to regulate, suspend or terminate your access, within their domain of authority, and you shall immediately comply with their instructions.

Operational Security Policies

Policies, example 2

[2] Herod clause:

[2] http://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/

Operational Security Policies

Policies, example 2

[2] Herod clause: *. . . the recipient agreed to assign their first born child to us for the duration of eternity.*

Its unlikely to find a similar clause in EGI Policies, still, get engaged, contribute, just stating I'm not bound by a policy does not really work.

[2] http://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/

Operational Security, Policies

Policies, EGI Security Incident Response Policy

https://documents.egi.eu/document/82

2. You shall promptly report suspected security incidents (or your involvement therein) that have known or potential impact or relationship to grid resources, services, or identities, via the incident response channels defined by the Grid.

Operational Security, Procedures

Components

- Policies (Define the pitch)
- Procedures (predicable actions)

Operational Security, Procedures

Procedures, Critical Vulnerability Handling Procedure

https://wiki.egi.eu/wiki/SEC03

For each RC who failed to comply to step 5, the EGI-CSIRT Security Officer on Duty temporarily suspends it from the infrastructure by setting the Certification Status of this RC to Suspended in GOC-DB. The EGI-CSIRT Security Officer on Duty will inform the NGI Security Officer and EGI Operations of this action.

Operational Security, Procedures

Procedures, Critical Vulnerability Handling Procedure

https://wiki.egi.eu/wiki/SEC01

What is expected to happen by when.

Operational Security

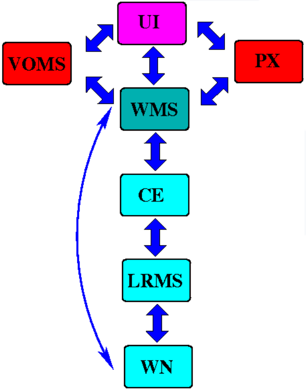
Components

- Policies (Define the pitch)
- Procedures
- Tools (IR)

Evolving distributed Infrastructure

Evolving distributed Infrastructure

WMS

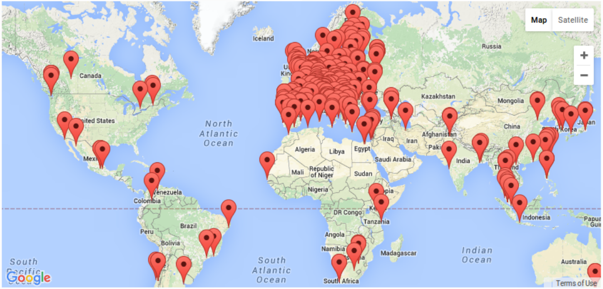


Operational Security, IR-Tools

Tools, stop account buse

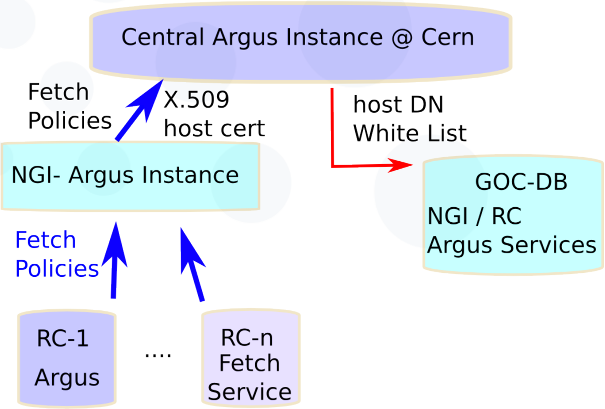
Operational Security, IR-Tools

Tools, stop account buse



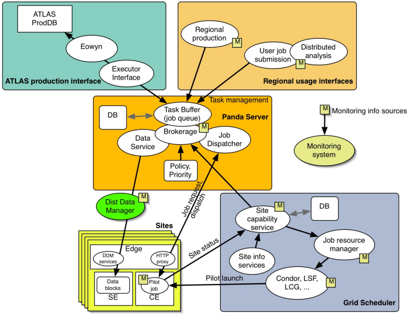
Operational Security, IR-Tools

Tools, stop account buse



Evolving distributed Infrastructure

VO-WMS, example, there are many



ATLAS ProdDB

Eowyn

Executor Interface

ATLAS production interface

Regional production

User job submission

Distributed analysis

Regional usage interfaces

Task management

DB

Task Buffer (job queue)

Panda Server

Brokerage

Data Service

Job Dispatcher

Policy, Priority

M Monitoring info sources

Monitoring system

Dist Data Manager

Job request, dispatch

Sites

Edge

DDM services

HTTP proxy

Data blocks

SE

Pilot job

CE

Site status

Pilot launch

Site capability service

DB

Job resource manager

Site info services

Condor, LSF, LCG, ...

Grid Scheduler

Operational Security, Tools II

Tools, stop account abuse

Operational Security, Evolving Policies

Policies, Traceability and Logging Policy

https://documents.egi.eu/document/81

. . . The aim is to be able to answer the basic questions who, what, where, and when concerning any incident. This requires retaining all relevant information, including timestamps and the digital identity of the user, sufficient to identify, for each service instance, and for every security event including at least the following: connect, authenticate, authorize (including identity changes) and disconnect. . . .

Operational Security, Traceability

Policies, Traceability and Logging Policy, Why ?

You need a password? . . . just kindly ask

I have shared a secure document with you via Google Docs.
Click to open: Document *http://some_url/file.php*
Google Docs makes it easy to create, store and share online documents, spreadsheets and presentations.
Thank you

Operational Security, IR VO-WMS

IR in changing environments demands close collaboration between the Security Teams

FedCloud Incidents / Issues in Incident Response (IR)

FedCloud Incidents

- Multiple Incidents, opportunistic compromises
- Vulnerable VA in appdb, Root compromise
- Vulnerable VA in appdb, tomcat compromise, used for DDOS attack

FedCloud IR tools

CERTIFIED BY TI TRUSTED INTRODUCER

Perun, Boris Parák (CESNET), Slávek Licehammer (Masaryk University)

- VMM & UM in Incident Response
- Goals: Stop/suspend VMs of suspended users
- Tool: Perun, Argus, Indigo (Andrea Ceccanti, INFN)

FedCloud IR Prevention

- Policies: https://documents.egi.eu/public/ShowDocument?docid=771 under review
- Goal: reduce attack surface by providing secured VM Images
- Automatized VM Image checking Daniel Kouřil (CESNET)

EGI-ENGAGE

CERTIFIED BY TI TRUSTED INTRODUCER

Federated Identities / Incident Response)

Federated Identity Roleplay

- Security Training Session Sunday afternoon
- about 10 experts discussing expected issues in Incident Handling
- interesting problems spotted, . . .