Assessment of the incident response processes in a Distributed Infrastructure

EGI CSIRT

SSC-19.03

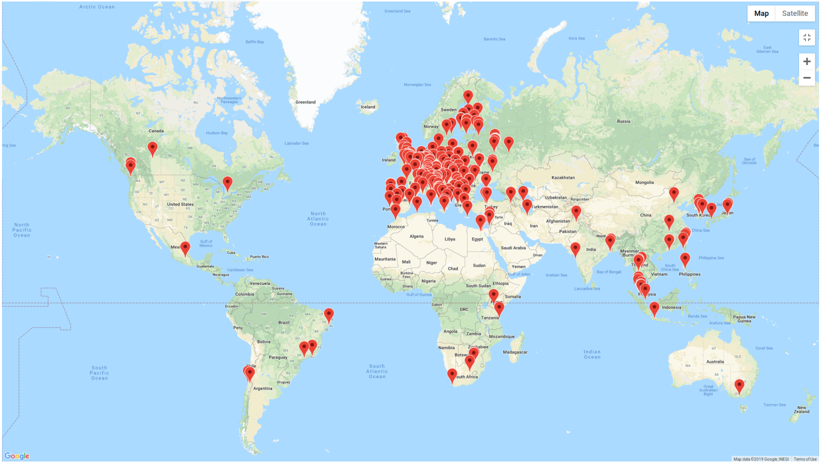
EGI CSIRT

CERTIFIED BY TI TRUSTED INTRODUCER

Developing Operational Security in Distributed Infrastructures

EGI: Advanced Computing for Research

EGI-CSIRT / Infrastructure Map



EGI CSIRT / Infrastructure Numbers

- current NGIs, Sites, ...https://goc.egi.eu/portal/
- Production Sites 450 (certified 343)
- NGIs 39 (some consist of multiple countries)

EGI CSIRT / Policy Framework

Policy Framework

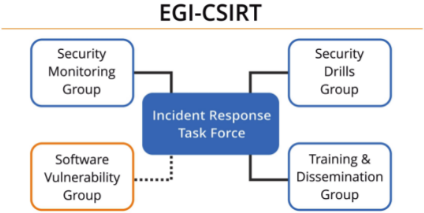
Policy framework in EGI provides CSIRT with:

- Have the infrastructure responsive to vulnerabilities
- Have the infrastructure ready to contribute in Incident Response (IR), logs etc
- Have the infrastructure to actively contribute in IR, information sharing
- Have a possibility to enforce actions (escalations)

EGI CSIRT / Operational Setup

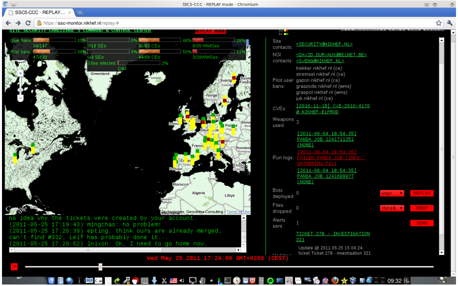
EGI-CSIRT Operational Setup

- Project wide coordination of operational security activities.
- Procedure / Policy development, testing these in . . .
- Security Service Challenges
- Security Monitoring
- Enforcing procedures/policies
- Allows for centralized tools (suspending IDs infrastructure wide, also on Christmas eve)
- Interfacing to other (Grid/NREN/VO) CSIRTs


EGI-CSIRT
Security Monitoring Group
Security Drills Group
Incident Response Task Force
Software Vulnerability Group
Training & Dissemination Group

EGI-CSIRT Operational Setup

- Project wide coordination of operational security activities.
- Procedure / Policy development, testing these in . . .
- Security Service Challenges
- Security Monitoring
- Enforcing procedures/policies
- Allows for centralized tools (suspending IDs infrastructure wide, also on Christmas eve)
- Interfacing to other (Grid/NREN/VO) CSIRTs



User bans: 37% 54/147 | 0% 0/19 SEs | 48% 45/93 CEs | 26% 9/35 WMSes

Pilot bans: 39% 47/120 | 0% 0/4 SEs | 50% 44/88 CEs | 11% 3/28WMSes

Sites infected: 2% 1/44

Site contacts: <SECURITY@NIKHEF.NL>

NGI contacts: <DAVID.DURVAUX@BELNET.BE> <SVENG@NIKHEF.NL>

Pilot user bans: trekker.nikhef.nl (ce)
stremsel.nikhef.nl (ce)
gazon.nikhef.nl (ce)
graszode.nikhef.nl (wms)
graspol.nikhef.nl (wms)
juk.nikhef.nl (ce)

CVEs: [2010-11-18] CVE-2010-4170 @ NIKHEF-ELPROD

Weapons used: 3

Run logs: [2011-06-04 18:54:35] PANDA JOB 1241711351 (NONE)
[2011-06-04 18:54:35] FAILED PANDA JOB (INFO : GATHERING FIL)
[2011-06-04 18:54:35] PANDA JOB 1241699977 (NONE)

Bots deployed: 0

Files dropped: 0

Alerts sent: 1

TICKET 278 - INVESTIGATION 321

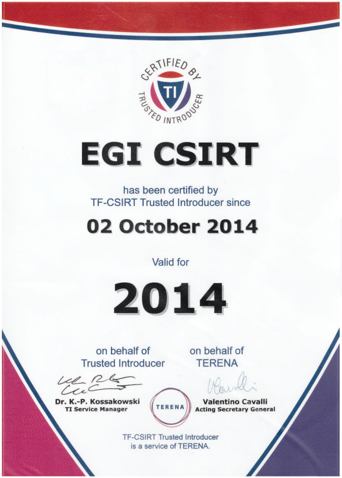
Update @ 2011-05-25 15:04:24: ticket Ticket 278 - investigation 321

```
no idea why the tickets were created by your account.
(2011-05-25 17:19:43) mingchao: no problem!
(2011-05-25 17:20:39) epting: think ours are already merged,
can't find #332, Leif has probably done it...
(2011-05-25 17:20:52) lnixon: OK, I need to go home now.
```

Wed May 25 2011 17:24:00 GMT+0200 (CEST)

Interfacing to other CSIRTs

TI, External Audit / Interfacing to other CSIRTs



EGI CSIRT

has been certified by
TF-CSIRT Trusted Introducer since

02 October 2014

Valid for

2014

on behalf of
Trusted Introducer

Dr. K.-P. Kossakowski
TI Service Manager

on behalf of
TERENA

Valentino Cavalli
Acting Secretary General

TF-CSIRT Trusted Introducer
is a service of TERENA.

- Numbers are constantly changing
- candidate (12)
- listed (119) (2009)
- accredited (97) (2012)
- certified (8) (2014)

Ready for an interactive self assessment? check: `https://check.ncsc.nl/questionnaire/`

EGI CSIRT Mission

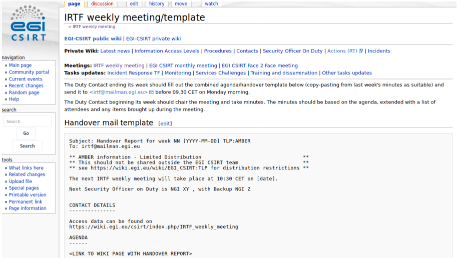
The EGI Computer Security and Incident Response Team (EGI-CSIRT) provides operational security for the EGI Infrastructure. This includes responding to computer security incidents affecting the infrastructure, which is carried out by co-ordinating the incident handling activities in the NGIs/EIROs, RCs, VOs, and where applicable interacting with partner Infrastructures CSIRTs and CSIRT communities with which EGI-CSIRT has a trust relationship.

https://documents.egi.eu/secure/ShowDocument?docid=385&version=12

Incident Prevention

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 6)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



IRTF weekly meeting/template

< IRTF weekly meeting

EGI-CSIRT public wiki | EGI-CSIRT private wiki

Private Wiki: Latest news | Information Access Levels | Procedures | Contacts | Security Officer On Duty | Actions (RT) | Incidents

Meetings: IRTF weekly meeting | EGI CSIRT monthly meeting | EGI CSIRT Face 2 Face meeting
Tasks updates: Incident Response TF | Monitoring | Services Challenges | Training and dissemination | Other tasks updates

The Duty Contact ending its week should fill out the combined agenda/handover template below (copy-pasting from last week's minutes as suitable) and send it to <irtf@mailman.egi.eu> before 09.30 CET on Monday morning.

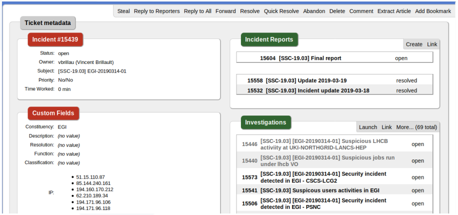
The Duty Contact beginning its week should chair the meeting and take minutes. The minutes should be based on the agenda, extended with a list of attendees and any items brought up during the meeting.

Handover mail template [edit]

```
Subject: Handover Report for week NN [YYYY-MM-DD] TLP:AMBER
To: irtf@mailman.egi.eu

** AMBER information - Limited Distribution                        **
** This should not be shared outside the EGI CSIRT team            **
** see https://wiki.egi.eu/wiki/EGI_CSIRT:TLP for distribution restrictions **

The next IRTF weekly meeting will take place at 10:30 CET on [date].

Next Security Officer on Duty is NGI XY , with Backup NGI Z


CONTACT DETAILS
---------------

Access data can be found on
https://wiki.egi.eu/csirt/index.php/IRTF_weekly_meeting

AGENDA
------

<LINK TO WIKI PAGE WITH HANDOVER REPORT>
```

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 6)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



Incident #15439

Status: open
Owner: vbrillau (Vincent Brillault)
Subject: [SSC-19.03] EGI-20190314-01
Priority: No/No
Time Worked: 0 min

Custom Fields

Constituency: EGI
Description: *(no value)*
Resolution: *(no value)*
Function: *(no value)*
Classification: *(no value)*
IP:
- 51.15.110.87
- 85.144.240.161
- 194.160.170.212
- 62.210.189.34
- 194.171.96.106
- 194.171.96.118

Incident Reports

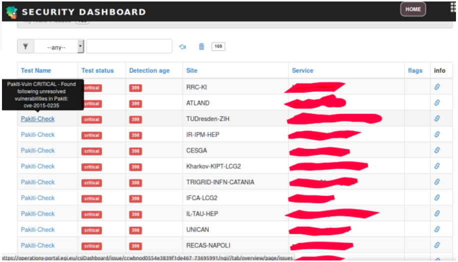
15604	[SSC-19.03] Final report	open
15558	[SSC-19.03] Update 2019-03-19	resolved
15532	[SSC-19.03] Incident update 2019-03-18	resolved

Investigations

15446	[SSC-19.03] [EGI-20190314-01] Suspicious LHCB activiity at UKI-NORTHGRID-LANCS-HEP	open
15440	[SSC-19.03] [EGI-20190314-01] Suspicious jobs run under lhcb VO	open
15573	[SSC-19.03] [EGI-20190314-01] Security incident detected in EGI - CSCS-LCG2	open
15541	[SSC-19.03] Suspicous users activities in EGI	open
15506	[SSC-19.03] [EGI-20190314-01] Security incident detected in EGI - PSNC	open

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 6)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



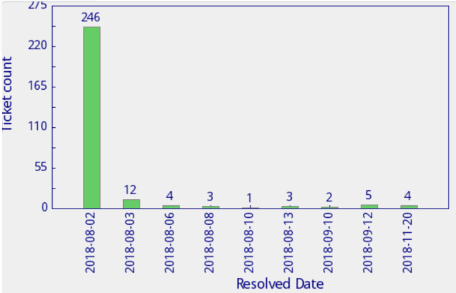
Pakiti-Vuln CRITICAL - Found following unresolved vulnerabilities in Pakiti: cve-2015-0235

Test Name	Test status	Detection age	Site	Service	flags	info
	critical	399	RRC-KI	[redacted]		🔗
	critical	399	ATLAND	[redacted]		🔗
Pakiti-Check	critical	399	TUDresden-ZIH	[redacted]		🔗
Pakiti-Check	critical	398	IR-IPM-HEP	[redacted]		🔗
Pakiti-Check	critical	398	CESGA	[redacted]		🔗
Pakiti-Check	critical	398	Kharkov-KIPT-LCG2	[redacted]		🔗
Pakiti-Check	critical	398	TRIGRID-INFN-CATANIA	[redacted]		🔗
Pakiti-Check	critical	398	IFCA-LCG2	[redacted]		🔗
Pakiti-Check	critical	398	IL-TAU-HEP	[redacted]		🔗
Pakiti-Check	critical	398	UNICAN	[redacted]		🔗
Pakiti-Check	critical	398	RECAS-NAPOLI	[redacted]		🔗

ttps://operations-portal.egi.eu/csiDashboard/issue/ccwbnod0554e3839f1de467_73695991/ngi//tab/overview/page/issues

EGI-CSIRT Incident Prevention

- Rota: Security Officer on Duty (IRTF members 6)
- Handover, follow up in RT-IR
- Security Dashboard: Results from Monitoring, SVG
- Communication end points in Goc-DB , ... are tested



Communication Challenge 2018

- First EGI-wide challenge (past challenges: NGI)
- Workflow similar to Trusted-Introducer challenges
- Verification of GOC-DB security contacts:
    - Using RT-IR: signed email, ticket accessible
    - Asking to click on a single link
- EGI Operation helping to recover broken contacts

Communication Challenge 2018 Results

- 23/272 clicks within 1 minute (8%)
- 101/272 clicks within 10 minutes (37%)
- 179/272 clicks within 1 hour (66%)
- **214/272 clicks within 4 hours (79%)**
- 234/272 clicks within 1 day (86%)
- 252/272 clicks within 4 days (93%)
- 261/272 clicks within 7+ days (96%)
- 2 clicks at 39 days...
- 9 without direct clicks

Working-hour wise, these numbers are even better!

Incident Response

Incident Response in EGI

Incidents: Incomplete list . . .

EGI-20150925-01	stole ssh user pw / root compromise / bitcoin mi
EGI-20150519-01	Vulnerable VA in appdb, Root compromise **clou**
EGI-20140113-01	BitCoin Mining **using grid technology**
EGI-20110418-01	stolen ssh credentials
EGI-20110301-01	bruteforce ssh **quite a few of this type**
EGI-20110121	web server misconfig
EGI-20100929-01	stolen ssh credentials
EGI-20100722	bruteforce ssh
EGI-20100707-01	stolen ssh credentials/remote vulns in CMSes
EGEE-20091204	stolen ssh credentials/X keyboard sniffing
GRID-SEC-001	stolen ssh credentials

Incident Response in EGI

Actions, Incident Response Procedure

- Incident is detected/reported, gets recorded in ticket sysem
- affected ResourceCenter(s) get contacted, asked for confirmation
- Warning / heads up gets issued infrastructure wide when needed
- Local team is responsible for incident resolution (close out report)
- EGI forensics experts support local team on request

Incident Response in EGI

Incidents: How they spread out . . .

- following IPs, tough . . . NRENS are good at that
- looking at layers 6/7 . . . Grid Security teams can provide **incident forecasts**

Security Service Challenges

Security Drills / Motivation

The objective:

The goal of the Security Service Challenges, is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available.

The challenges address communication, containment (access control) and forensics.

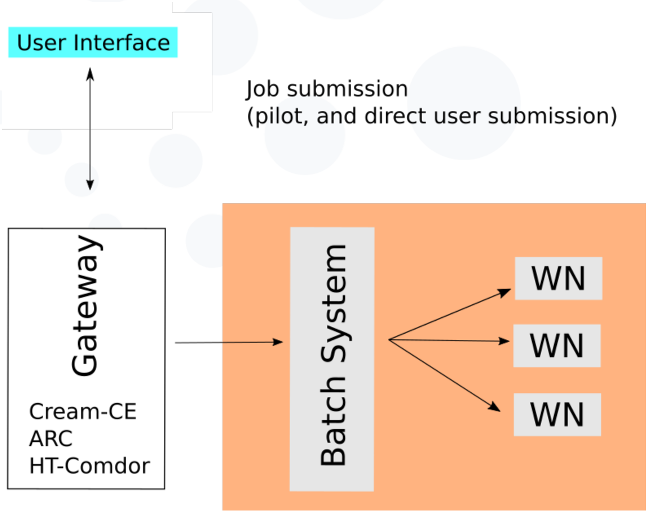
The Challenge, Preparations

- First discussions with LHCB VO at isgc-2018
- F2F meetings with LHCB/EGI CSIRT
- Align possible IR actions among the security teams. The security teams should act in a predictable way.
- Which information is needed by who, and how can the information be retrieved.
- Announcements at GDB/OMB

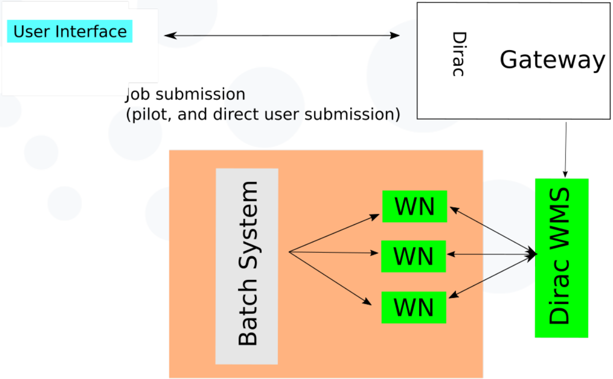
The Challenge, SetUp and Roles

- Incident Coordinator (+ forensics expertise): EGI CSIRT
- Incident handling to be done as ”business as usual”. Security Officer on Duty, Security Contacts at sites and VO.
- Observers (from VO, and EGI CSIRT), know all details of the exercise, only step in when needed.
- Attacker, send malicious jobs, ”control” the bots, ”add noise” to the exercise when needed.
- ”Victims”: 1 User
- Incident Responders: CSIRTs at VO and Sites

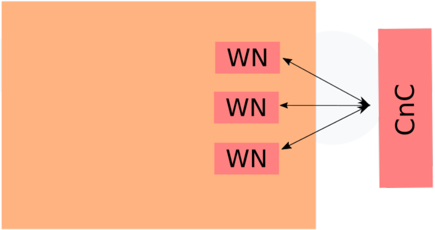
Security Drills Challenge Generic Job submission



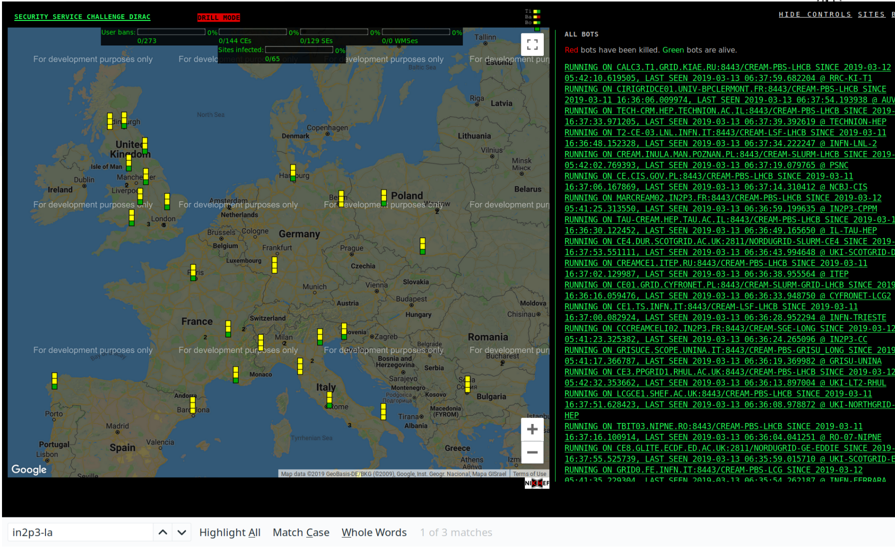
Security Drills Challenge Job submission



Security Drills TakeOver



Security Drills TakeOver



User bans: 0% 0/273 | 0% 0/144 CEs | 0% 0/129 SEs | 0% 0/0 WMSes

Sites infected: 0% 0/65

ALL BOTS

Red bots have been killed. Green bots are alive.

```
RUNNING ON CALC3.T1.GRID.KIAE.RU:8443/CREAM-PBS-LHCB SINCE 2019-03-12
05:42:10.619505, LAST SEEN 2019-03-13 06:37:59.682204 @ RRC-KI-T1
RUNNING ON CIRIGRIDCE01.UNIV-BPCLERMONT.FR:8443/CREAM-PBS-LHCB SINCE
2019-03-11 16:36:06.009974, LAST SEEN 2019-03-13 06:37:54.193938 @ AUV
RUNNING ON TECH-CRM.HEP.TECHNION.AC.IL:8443/CREAM-PBS-LHCB SINCE 2019-
16:37:33.971205, LAST SEEN 2019-03-13 06:37:39.392619 @ TECHNION-HEP
RUNNING ON T2-CE-03.LNL.INFN.IT:8443/CREAM-LSF-LHCB SINCE 2019-03-11
16:36:48.152328, LAST SEEN 2019-03-13 06:37:34.222247 @ INFN-LNL-2
RUNNING ON CREAM.INULA.MAN.POZNAN.PL:8443/CREAM-SLURM-LHCB SINCE 2019-
05:42:02.769393, LAST SEEN 2019-03-13 06:37:19.079765 @ PSNC
RUNNING ON CE.CIS.GOV.PL:8443/CREAM-PBS-LHCB SINCE 2019-03-11
16:37:06.167869, LAST SEEN 2019-03-13 06:37:14.310412 @ NCBJ-CIS
RUNNING ON MARCREAM02.IN2P3.FR:8443/CREAM-PBS-LHCB SINCE 2019-03-12
05:41:25.313550, LAST SEEN 2019-03-13 06:36:59.199635 @ IN2P3-CPPM
RUNNING ON TAU-CREAM.HEP.TAU.AC.IL:8443/CREAM-PBS-LHCB SINCE 2019-03-1
16:36:30.122452, LAST SEEN 2019-03-13 06:36:49.165650 @ IL-TAU-HEP
RUNNING ON CE4.DUR.SCOTGRID.AC.UK:2811/NORDUGRID-SLURM-CE4 SINCE 2019-
16:37:53.551111, LAST SEEN 2019-03-13 06:36:43.994648 @ UKI-SCOTGRID-D
RUNNING ON CREAMCE1.ITEP.RU:8443/CREAM-PBS-LHCB SINCE 2019-03-11
16:37:02.129987, LAST SEEN 2019-03-13 06:36:38.955564 @ ITEP
RUNNING ON CE01.GRID.CYFRONET.PL:8443/CREAM-SLURM-GRID-LHCB SINCE 2019
16:36:16.059476, LAST SEEN 2019-03-13 06:36:33.948750 @ CYFRONET-LCG2
RUNNING ON CE1.TS.INFN.IT:8443/CREAM-LSF-LHCB SINCE 2019-03-11
16:37:00.082924, LAST SEEN 2019-03-13 06:36:28.952294 @ INFN-TRIESTE
RUNNING ON CCCREAMCELI02.IN2P3.FR:8443/CREAM-SGE-LONG SINCE 2019-03-12
05:41:23.325382, LAST SEEN 2019-03-13 06:36:24.265096 @ IN2P3-CC
RUNNING ON GRISUCE.SCOPE.UNINA.IT:8443/CREAM-PBS-GRISU_LONG SINCE 2019
05:41:17.366787, LAST SEEN 2019-03-13 06:36:19.369982 @ GRISU-UNINA
RUNNING ON CE3.PPGRID1.RHUL.AC.UK:8443/CREAM-PBS-LHCB SINCE 2019-03-12
05:42:32.353662, LAST SEEN 2019-03-13 06:36:13.897004 @ UKI-LT2-RHUL
RUNNING ON LCGCE1.SHEF.AC.UK:8443/CREAM-PBS-LHCB SINCE 2019-03-11
16:37:51.628423, LAST SEEN 2019-03-13 06:36:08.978872 @ UKI-NORTHGRID-
HEP
RUNNING ON TBIT03.NIPNE.RO:8443/CREAM-PBS-LHCB SINCE 2019-03-11
16:37:16.100914, LAST SEEN 2019-03-13 06:36:04.041251 @ RO-07-NIPNE
RUNNING ON CE8.GLITE.ECDF.ED.AC.UK:2811/NORDUGRID-GE-EDDIE SINCE 2019-
16:37:55.525739, LAST SEEN 2019-03-13 06:35:59.015710 @ UKI-SCOTGRID-E
RUNNING ON GRID0.FE.INFN.IT:8443/CREAM-PBS-LCG SINCE 2019-03-12
05:41:35.229304, LAST SEEN 2019-03-13 06:35:54.262187 @ INFN-FERRARA
```

in2p3-la   Highlight All   Match Case   Whole Words   1 of 3 matches

Security Drills TakeOver

The take over is not really trivial :-) how we did it will be in the next presentation.

SSC Dirac

The Challenge

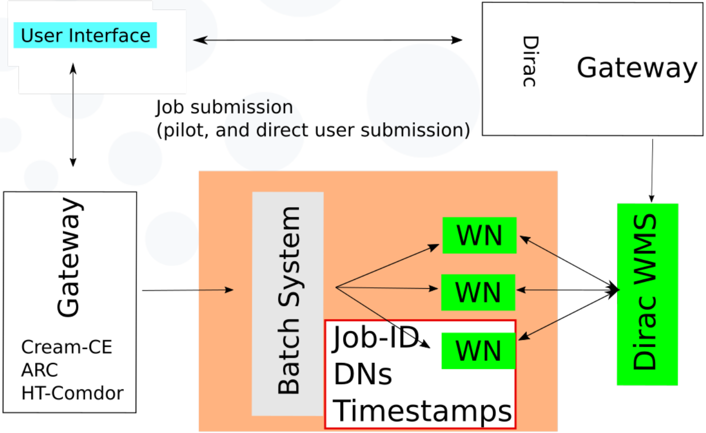
Challenge

Respond to the above created situation

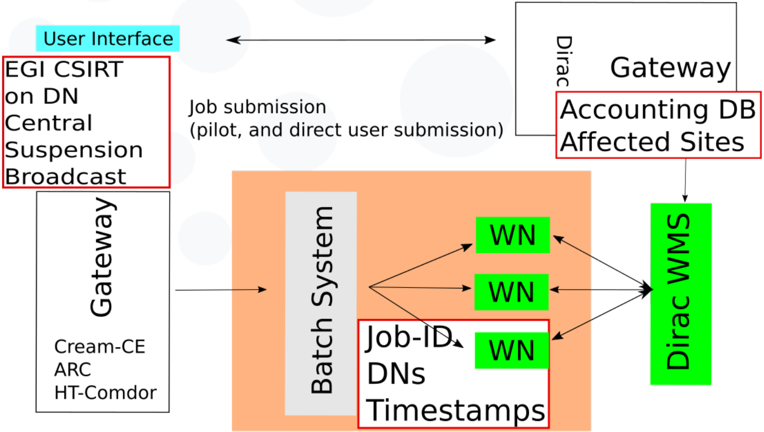
The Challenge

- Observe/Orient
  - Confirm it is an incident.
  - Find out what is the extent of the incident
  - Which DNs are involved, which DNs have to be suspended.
- Decide/Act Stop the incident from further spreading
  - Suspend the DN, prevent more malicious jobs started.
  - Stop malicious jobs
  - Understand the latencies of the various countermeasures.
- Understand the incident, forensics needed.

Security Drills Info gathering



Security Drills IR actions



The Challenge, Timeline I

- 11. March: Submitting jobs to Dirac, and direct submission
- 12. March: Announcement
- 13. March: Report from 1 site, ”we saw uncommon activity”
- 14. March: VO informed
- 14. March: One more similar reports received.
- 15. March: adding noise to the incident (miner + dos)
- 15. March: Site is reporting: Problematic UI is LBvobox, user: ”Pilot submitter”.
- 15. March: 15:15 Broadcast: we have an incident.

The Challenge, Timeline II

- 15.03 15:20 Sites suspend Pilot submitter (this appears to be the miscreant)
- 15.03 16:10 SurfCERT informs Nikhef that they are under attack
- 15.03 16:20 Sites see the implications of suspending the pilot submitter. (”Suspending the VO”)
- 15.03 16:30 Sites report the dos script
- 15.03 23:10 last contribution for that day
- 16.03 08:25 additional feedback from one site.

The Challenge, Timeline II

- 18.03 Weekly Meeting: agreed to not interfere with SSC-19.03
- 22.03 End of SSC-19.03 announced, welcoming the final reports.
- 01.04 Evaluation started.

The Challenge, Debriefing

- **A lot of data, just started**
- Evaluation/Scoring of the sites performance.
- Site Reports, Reports to *Board.
- Check deployed sensors.
- Hands on training.
- Revisit Procedures, Operational tools