EGI CSIRT Security Service Challenge in LHCB DIRAC, SSC-19.03

EGI CSIRT

GDB 8 May 2019

EOSC-hub

Goal of the Assessment of the IR processes

Goal

Goal: Answer to the questions, what is the overall security situation?, how well are the different IRprocedures interfaced to each other?, what are the pitfalls?

Boundary Conditions

- According to our policies: Security is a site decision
- EGI CSIRT coordinates operational security activities
- Practicalities:
  - Who has access to which information
  - who has access to which access controls
- Can one security team deal with an incident involving compromised credentials? $\rightarrow$ **No!**:w

EGI CSIRTs IRTF, in brief

in final report

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.

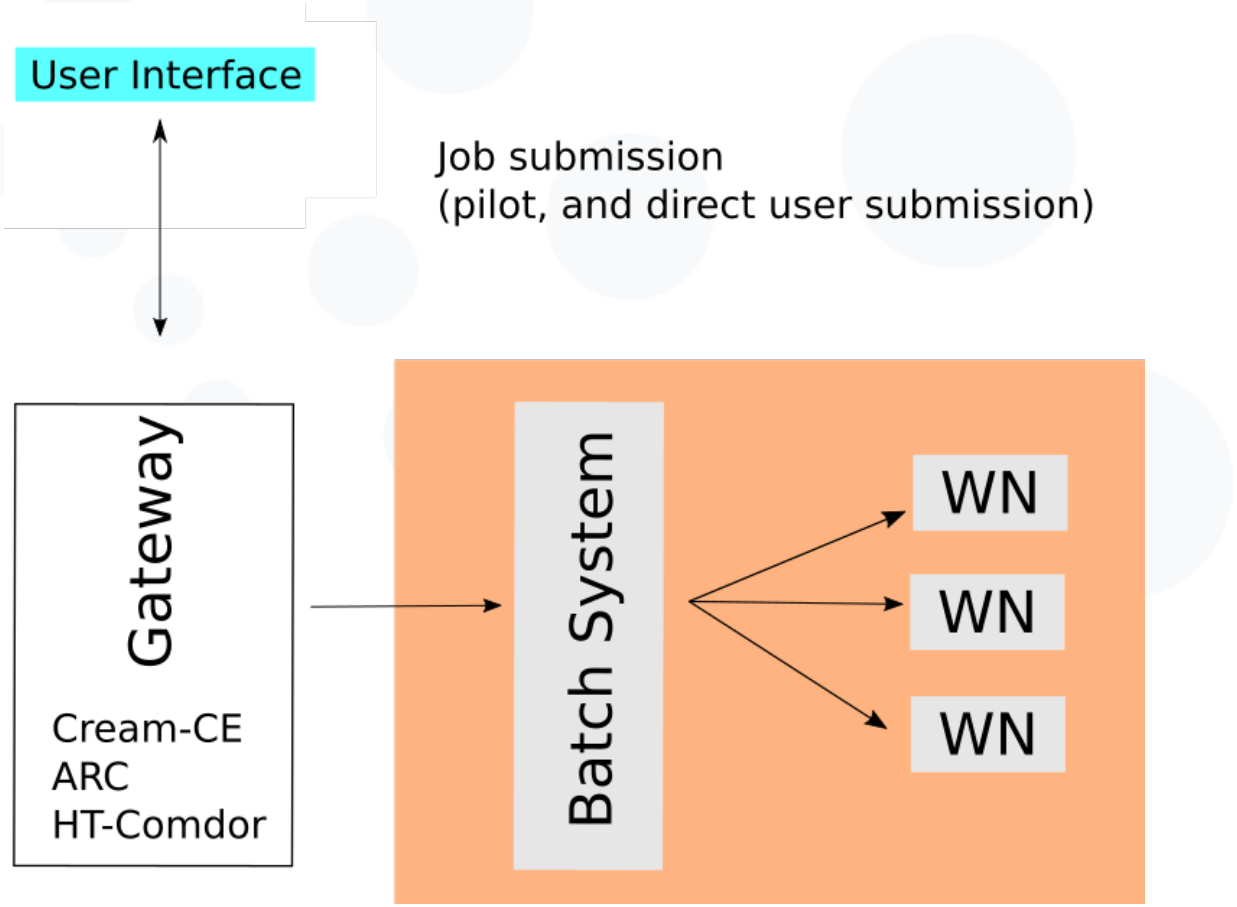
The Challenge, Preparations

- 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

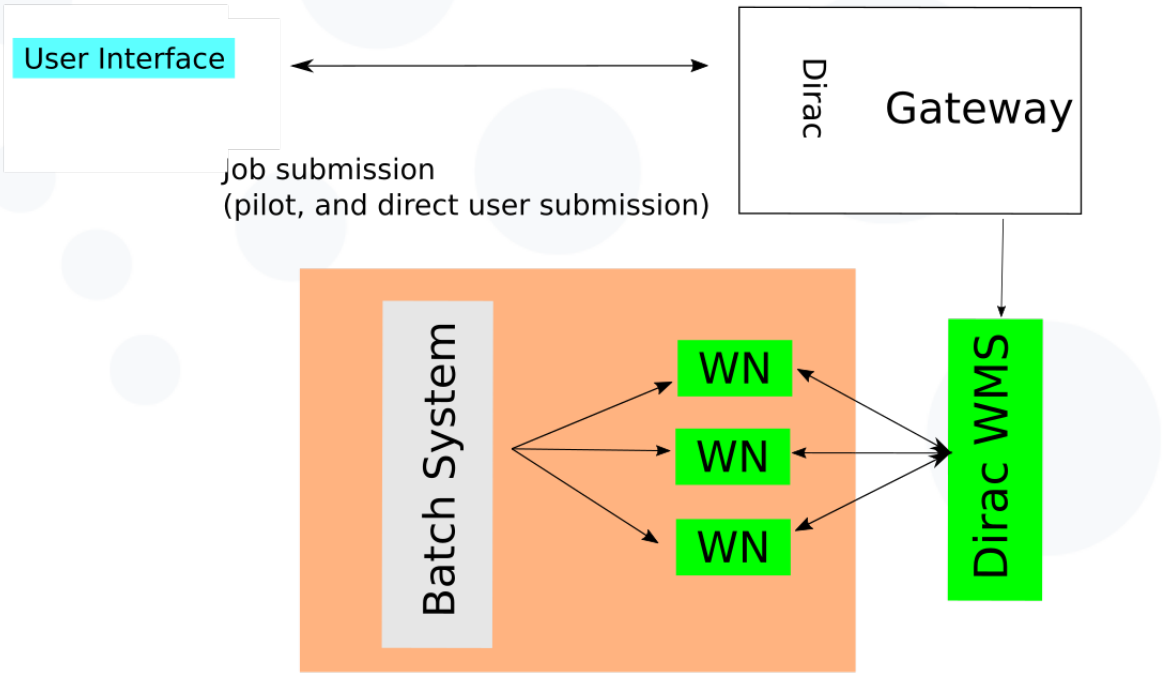
The Challenge, SetUp and Roles

- 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

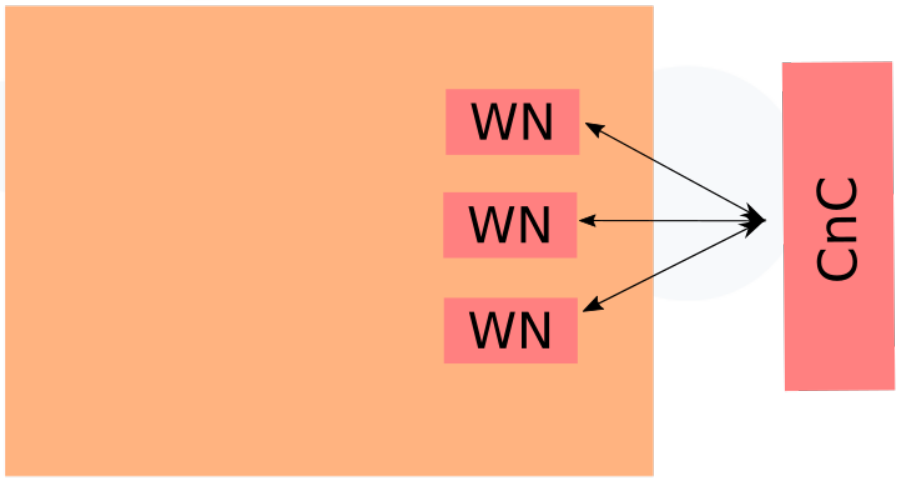
Security Drills Challenge Generic Job submission



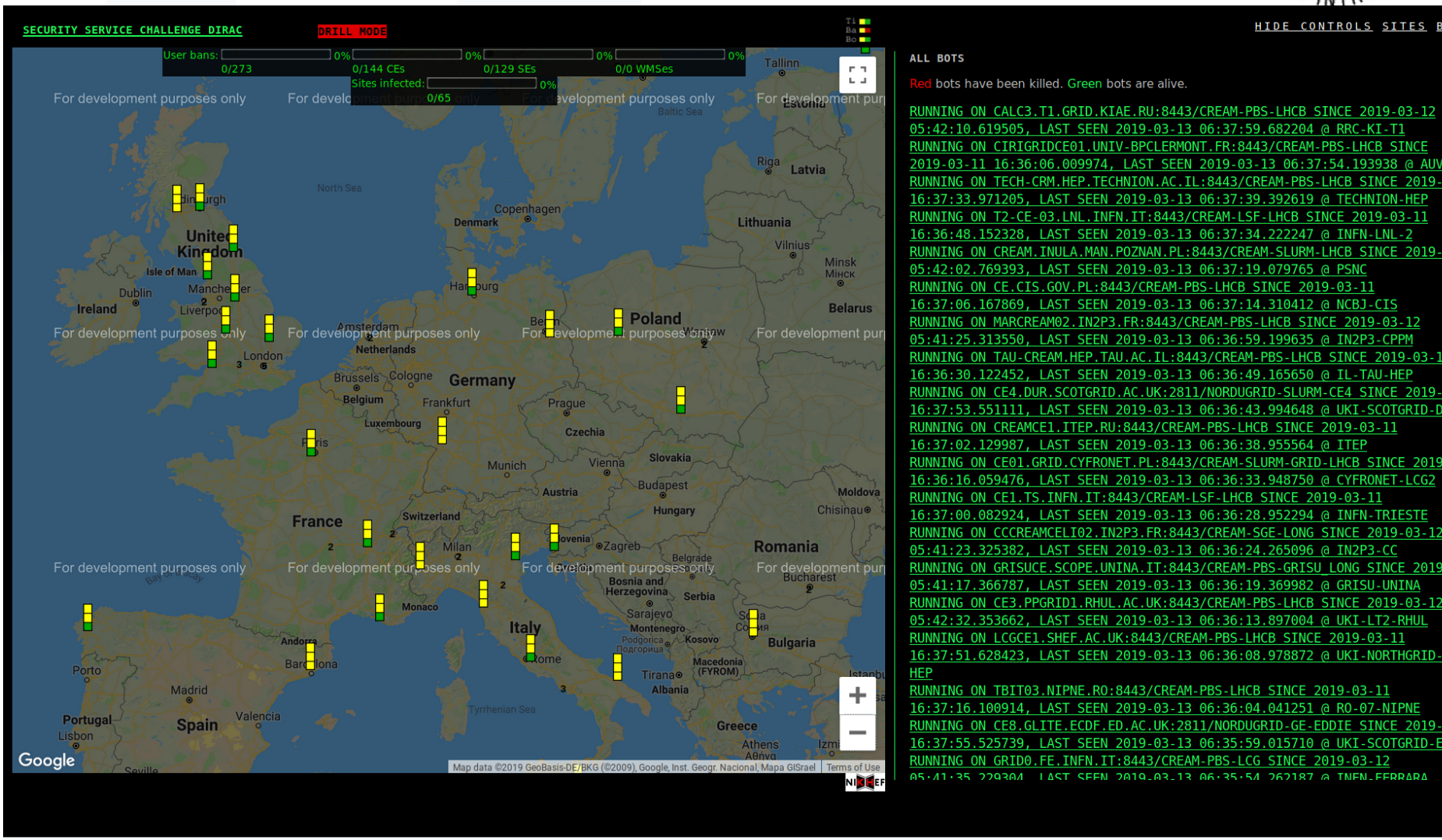
Security Drills Challenge Job submission



Security Drills TakeOver



Security Drills TakeOver



Security Drills TakeOver

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

SSC Dirac

SSC-19.03
The Situation

Situation

- Someone massively submitted malware through accepted channels.
- Malware creates a botnet, CnC hidden behind TOR.
- Botnet can take malicious actions:
  - *Crypto-currency mining* (heavy CPU load)
  - DDOS against remote targets

The Challenge

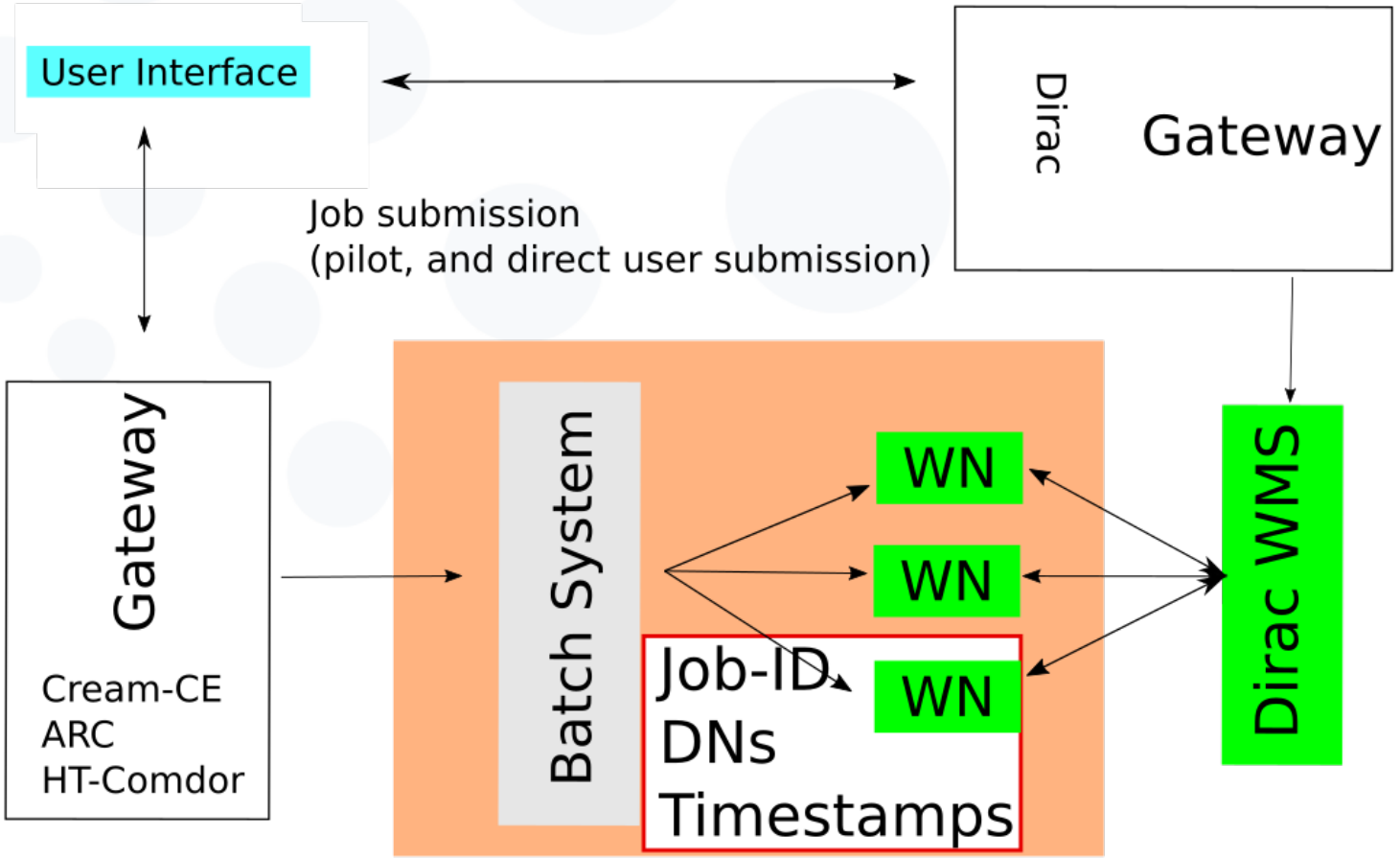
Challenge

Respond to the above created situation

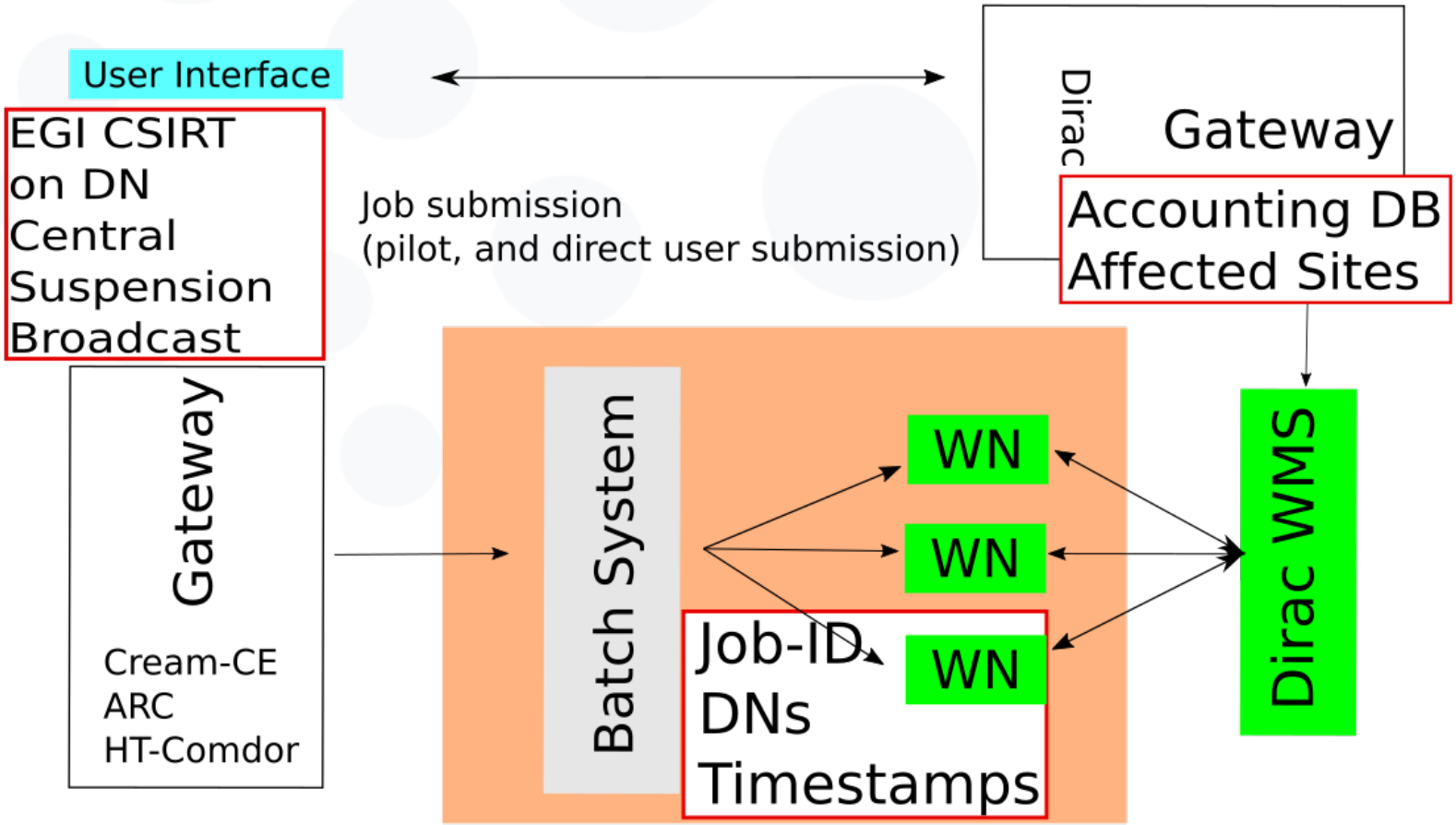
The Challenge

- 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



SSC-19.03 Timeline I

- 11. March: Submitting jobs (direct & through VO)
- 12. March: SSC announcement, contact check
- 13. March: Site report: *we saw uncommon activity*
- 14. March: VO informed
- 14. March: One more similar report received
- 15. March: adding noise to the incident (miner + ddos'ing Nikhef)
- 15. March: Site is reporting: Problematic UI is LBvobox, user: "Pilot submitter"
- 15. March: 15:15 Broadcast: we have an incident

SSC-19.03 Timeline II

- 15.03 15:20 Sites suspend Pilot submitter (this appears to be the miscreant)
- 15.03 16:10 SurfCERT informs Nikhef that Nikhef is 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.

SSC-19.03 Timeline III

- 18.03 IRTF weekly meeting: agreed to not interfere
- 22.03 End of SSC-19.03 announced, welcoming the final reports
- 01.04 Evaluation started

Digging for data, ...

Evaluation information sources: SSC-Monitor logs, RT-IR tickets

A lot of data, analysis started, started to extract data to find . . .

SSC-19.03
Preliminary results

Communications:

- X Percent within target time.
- Y Nr of sites with broken communication channel.
- Crucial inter-csirt communication **not** sufficient.

SSC-19.03
Preliminary results

Containment:

- Shortest(best) time to stop processes: average: longest:
- Shortest(best) time to suspend user: average: longest:
- X Percent of the sites suspended the pilot job submitter, effectively suspending the VO.

SSC-19.03
Preliminary results

Forensics:

- Highest score:
- Average score:
- Lowest score:
- X Percent of sites provided malware samples

Note: full Forensics are not expected, basic actions (including memory dump) are needed to fully solve this challenge. This will be addressed in the hands-on training (parallel session)

SSC-19.03 Debriefing

- From a first glance at the sites responses, less good than SSC-4
- Bots still living after extended time.
- Some sites did not respond as expected.

SSC-19.03 Debriefing

- Evaluation/Scoring of the sites performance.
- Site Reports, Reports to *Board.
- Check deployed sensors. (What does the SOC see?)
- Hands on training. (Tuesday)
- Revisit Procedures, Operational tools
- Redo the exercise addressing the identified issues.

Any question?