

# A BRAINSTORMING ON SECURITY FIRE DRILLS

**Classification, Feasibility, Usefulness and Implications**

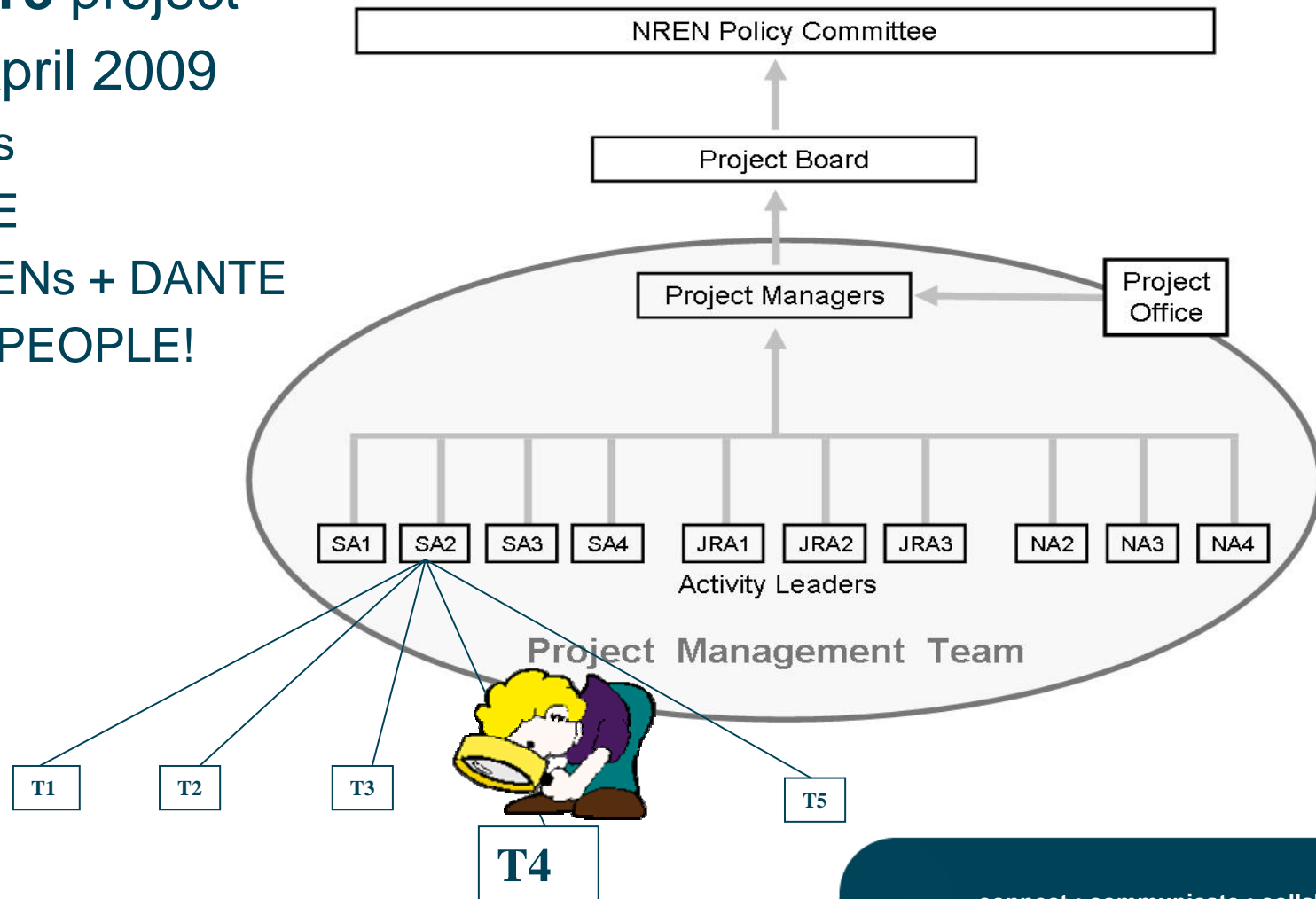
Maurizio Molina, DANTE – Nino Jogun, CARNET  
on behalf of GÉANT3 project, SA2/T4

TF-CSIRT, Tallin, 25<sup>th</sup> Sep. 2009

# Where this work originates: SA2/T4



- SA2/T4 – “Multi Domain Security Service” in **GÉANT3** project
- Started April 2009
  - 4 Years
  - ≈ 6 FTE
  - 14 NRENs + DANTE
  - CERT PEOPLE!



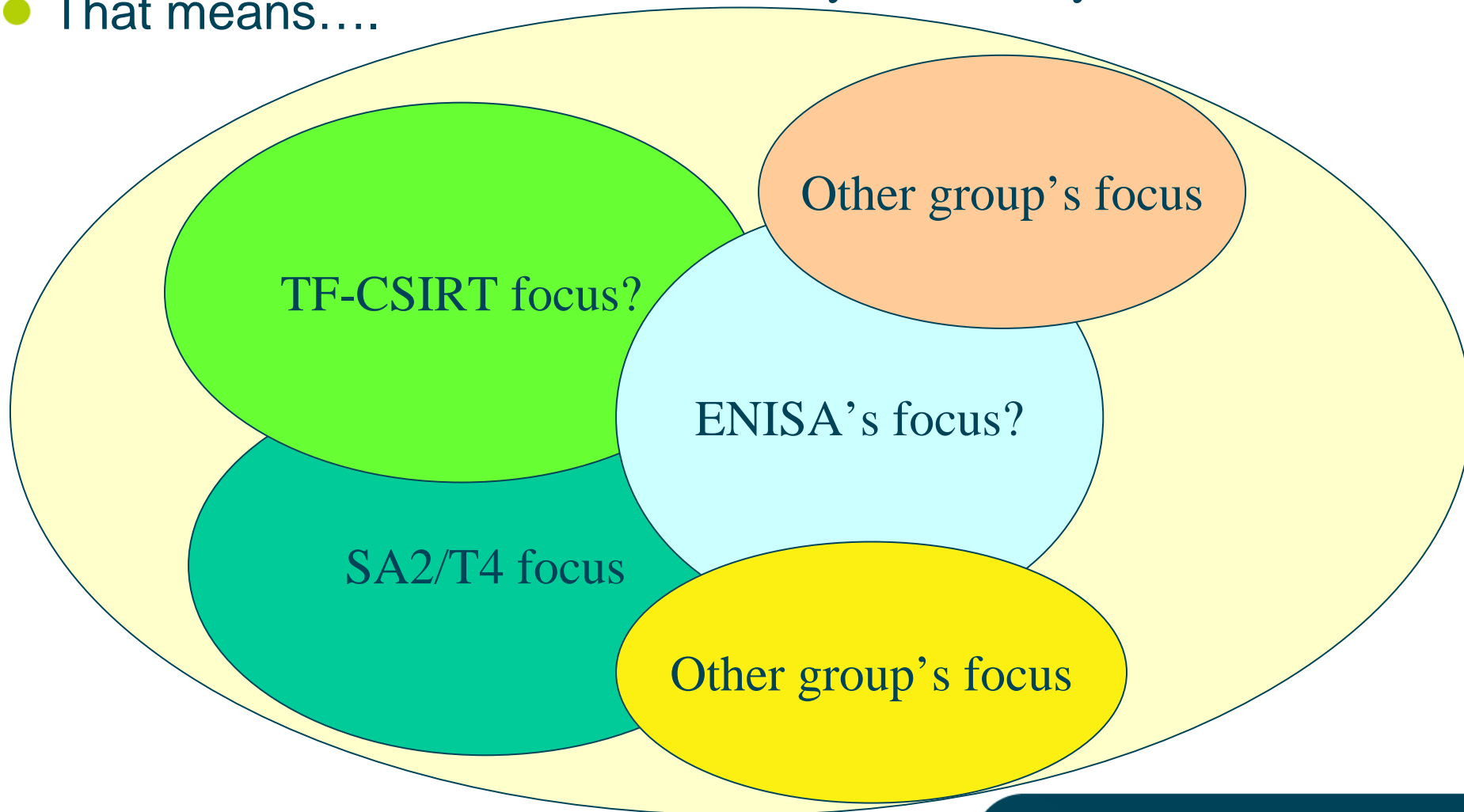
- SA2/T4 Focus is security of Multi Domain services in GÉANT3
  - Monitoring services (perfSONAR)
  - Automatic L2 and Wavelength setup (AutoBahn)
  - ...
- A lot of in-house coding for the above services
- SA2/T4 must assist in all phases (design, coding, deployment, operation)
- For the latter, we have “Security Fire Drills (S.F.D.)” in our workplan
- SFD is also in TF-CSIRT and other entities’ charter
- We want to share ideas, experiences, procedures and tools for implementing SFD
  - And learn from who already did something!

# Just remember our focus: Multi Domain services on GEANT3



## “Universe” of Cyber Security Fire Drills

- That means....



# Starting point: the S.F.D. matrix



Things to consider about S.F.D.

- Feasibility
- Usefulness
- Implications

Classification of S.F.D.

	Feasibility		Usefulness			Implications	
Type 1							
Type 2							
Type 3							
...							
...							
Type n							

The content!

- Host perimeter S.F.D.

- Testing the security resilience of applications and servers
- Testing how service owners, administrators and CERTs discover, handle and (possibly) mitigate security issues

- Network perimeter S.F.D.

- Testing how NOCs and CERTs detect and handle “incidents” involving one or more networks, and possibly mitigate them

## Classification: what we did not consider (because out of SA2/T4 scope)



- We did not consider the two “extrema”
- The “end user” case
  - Password strength
  - social engineering, phishing
  - Copyright infringements, illegal material
- The “network resilience” case
  - Simulation of attacks on NW infrastructure with link saturation
    - *Who will ever give authorization for that???*
  - However, if some GN3 multi-domain services are compromised, network performances may be affected (AutoBahn, perfSONAR)

# Classification: Host perimeter S.F.D.



Type	Description
System ( <u>partly</u> announced)	attack a system and successfully compromise it (without sys admin knowing)
System ( <u>fully</u> announced)	attack a system exploiting some privileged access, in coordination with system administrator
Service ( <u>partly</u> announced)	attack a service and successfully compromise it (without service owner knowing)
Service ( <u>fully</u> announced)	Attack a service in coordination and with additional info given by service owner

=> Service: distributed application and associated communication protocols

# Classification: Network perimeter S.F.D.



Type	Description
Real traffic injection	(D)DoS attack on specific service, or ethical worm
Monitoring alert injection	Make network monitoring system produce fake alerts
Network Incident Handling test	Craft incident report (cross-organization) (but no real traffic, no fake monitoring tools alerts)

⇒ We assume all these tests must be “partly announced”

## ● Feasibility

- What are the required resources, knowledge and authorizations to carry them out?

## ● Usefulness

- What are the goals?
- What are the criteria defining a successful test?
- What are the factors that may cause the test to be unreliable / not significant?

## ● Implications

- Who can be "disturbed" by the test?
- What legal issues you and those giving you authorization need to be aware of?

# Host perimeter S.F.D. - Feasibility



Type	Require
1a) System (partly announced)	An <b>exploitable vulnerability</b> in the system, idea of what to do when access is gained (e.g. manipulate logs, create additional accounts, open backdoors etc.); <b>Authorization; one or more informed persons in escalation chain</b>
1b) System (fully announced)	<b>access</b> to the system, idea of what to do when access is gained (see above), coordination with system admin; <b>Authorization</b>
2a) Service (partly announced)	As 1a) but vulnerability is sought in specific application, and <b>service owner <math>\neq</math> sys admin</b>
2b) Service (fully announced)	As 1b) but vulnerability is sought in specific application, and <b>service owner <math>\neq</math> sys admin</b>

Type	Require	
Real traffic injection	network bandwidth, traffic generators, fake malware traffic emulator;	Authorization; one or more informed persons in escalation chain
Monitoring alert injection	access to monitoring systems (IDS, IPS, NetFlow, log processing...), injection of fake network events in them;	
Network Incident Handling test	mail client; fake evidence generator;	

# Host perimeter S.F.D. - Usefulness



Type	Goal	Success criteria	Failure/test bias risks
1a) System (partly announced)	<b>resilience</b> of system to attacks; <u>or (if sys compromised):</u> effectiveness of system monitoring and <b>admin IH capabilities</b>	<b>no vulnerability</b> found or exploited; <u>or (if sys compromised):</u> <b>admin detects and fixes/escalates</b> in reasonable time	not enough knowledge to find or exploit a vulnerability, but <b>system may still be compromised by others;</b>
1b) System (fully announced)	effectiveness of system monitoring and <b>admin IH capabilities</b>	<b>admin detects and fixes/escalates</b> in reasonable time	admin may <b>not pay attention and lower guards</b> in general
2a) Service (partly announced)	as 1a), but <b>service owner</b> also involved	as 1a), but <b>service owner</b> also involved	as 1a), but <b>service owner</b> also involved
2b) Service (fully announced)	as 1b), but <b>service owner</b> also involved	as 1b), but <b>service owner</b> also involved	as 1b), but <b>service owner</b> also involved

# Network perimeter S.F.D. - Usefulness



Type	Goal	Success criteria	Failure/test bias risks
Real traffic injection	effectiveness of <b>network monitoring</b> systems and net admin <b>IH capabilities</b>	service <b>resilient</b> to attack; virus/worm not spreading; netw. <b>monitoring</b> system detecting; netw. <b>admin fix/escalate</b> quickly	Traffic injection below threshold of monitoring system, <b>no action taken</b> ; traffic filtered by intermediate networks
Monitoring alert injection	net admin <b>IH capabilities</b> ; ability to <b>cross check internal evidence</b> (difficult!!)	Netw. <b>admin fix/escalate</b> quickly	Different monitoring systems; <b>impossible to create of fake alerts</b> ; possible bias if who opens access to monitoring systems is involved in test
Network Incident Handling test	net <b>admin IH capabilities</b> ; ability to <b>cross check external evidence</b> (easier!!)	network <b>admins react</b> in reasonable time <b>but cross check evidence</b> and take no action	<b>Low risks</b> of test failure, test is simple and well defined

# Host perimeter S.F.D. - Issues



Type	Impact (who is “disturbed”)	Legal issues
1a) System (partly announced)	<b>system admins, users</b> (if production system), <b>CSIRT</b> (if detected and esalated)	"unauthorised access to computers" is normally a <b>criminal offence</b> . Need to be very sure you have <b>authority</b> from the <b>right people</b> . Also if you actually compromise a system there may be <b>Data Protection implications</b> (mandatory notification of security breaches in some countries). Depending on the impact of your compromise, there may be liability issues
1b) System (fully announced)	<b>system admins, CSIRT</b> (if detected and esalated); <b>user</b> impact can be controlled	As above. Given the data protection implications, <b>sysadmins may not be the appropriate persons to give AuthZ</b>
2a) Service (partly announced)	as 1a) + <b>service owner</b>	As 1a)
2b) Service (fully announced)	as 1b) + <b>service owner</b>	As 1b)

# Network perimeter S.F.D. - Issues



Type	Impact (who is “disturbed”)	Legal issues
network test, real traffic	possible widespread <b>collateral damage</b> due to e.g. link saturation or filter setup (attack completion); <b>users</b> (if production service), <b>network admins, CSIRT</b> (one or more Networks)	<b>DoS attacks are generally crimes.</b> If you use a bot to launch DDoS it’s the unauthZ use of these computers that is a crime, (even having the consent of the eventual target). Releasing a worm or virus is also a crime: <b>authZ is vital</b> , but must be very sure that it’ll only spread to machines where you have authority
network test, no traffic but fake monitoring system alerts	<b>network admins, CSIRT;</b> <b>users</b> affected if admins set filters	<b>Small risk</b> of committing unauthorised access/modification offences here
pure network Incident Handling test	<b>network admins, CSIRT;</b> <b>users affected</b> if admins set filters (if do not cross check evidence)	<b>Small risk:</b> potential liability for wasting people's time, lost work etc

- SA2/T4 next step is reviewing the SFD Matrix, exclude the unfeasible tests, prioritise the others, and then move towards implementation
  - We would value your feedback here
  - Also: did we miss entire ROWs or COLUMNS?
- What is TF-CSIRT position? I.e.: what is the overlap of TF-CSIRT with SA2/T4 in this area? How can TF-CSIRT benefit from what we do?
- ENISA's position?

- [Maurizio.molina@dante.net](mailto:Maurizio.molina@dante.net)
- ML: [gn3-sa2-t4@geant.net](mailto:gn3-sa2-t4@geant.net) (subscriber only, but I will get and approve non-member posting...)
- Many thanks to Andrew Cormack!