All is calm at your local security team. Too calm.
Hmmm. This user is acting very strangely.

It's one of our external users, coming in through eduGAIN.

Which user?

Think they're compromised? Can we reach security at their home organisation?

No! All we have is a billing contact...
... an incident spread throughout the federated R&E community via a single compromised identity?
Federated Security Incident Response

The problem

• Clearly an inviting vector of attack
• The lack of a centralised support system for security incident response is an identified risk to the success of eduGAIN
• We will need organisations to collaborate during incident response – this may be outside their remit
Federated Security Incident Response

The solution

• Attacks are inevitable 😞
• But we can make security capability transparent and build relationships between organisations and people 😊

We need a Security Incident Response Trust Framework for Federated Identity, Sirtfi!
Who’s doing the work?

- **REFEDS** Working Group
- Groundwork done by the **AARC** Project
- Handover to GN4 for deployment

Who will be the first to benefit?

- Pilot federations
- Key e-Infrastructures
- Several new services adding Sirtfi as a requirement
Want to find out more?
https://refeds.org/sirtfi

We have a poster at TNC!

Want to join? Visit our Wiki

Curious? Visit our homepage
Thank you

Any Questions?

hannah.short@cern.ch