Security Service Challenge 23.03, Crossing borders, the bigger picture

SSC-23.03, CMS VO

Sven Gabriel sveng@nikhef.nl, Nikhef, EGI-CSIRT,
Head Chief Experts

21. June 2023

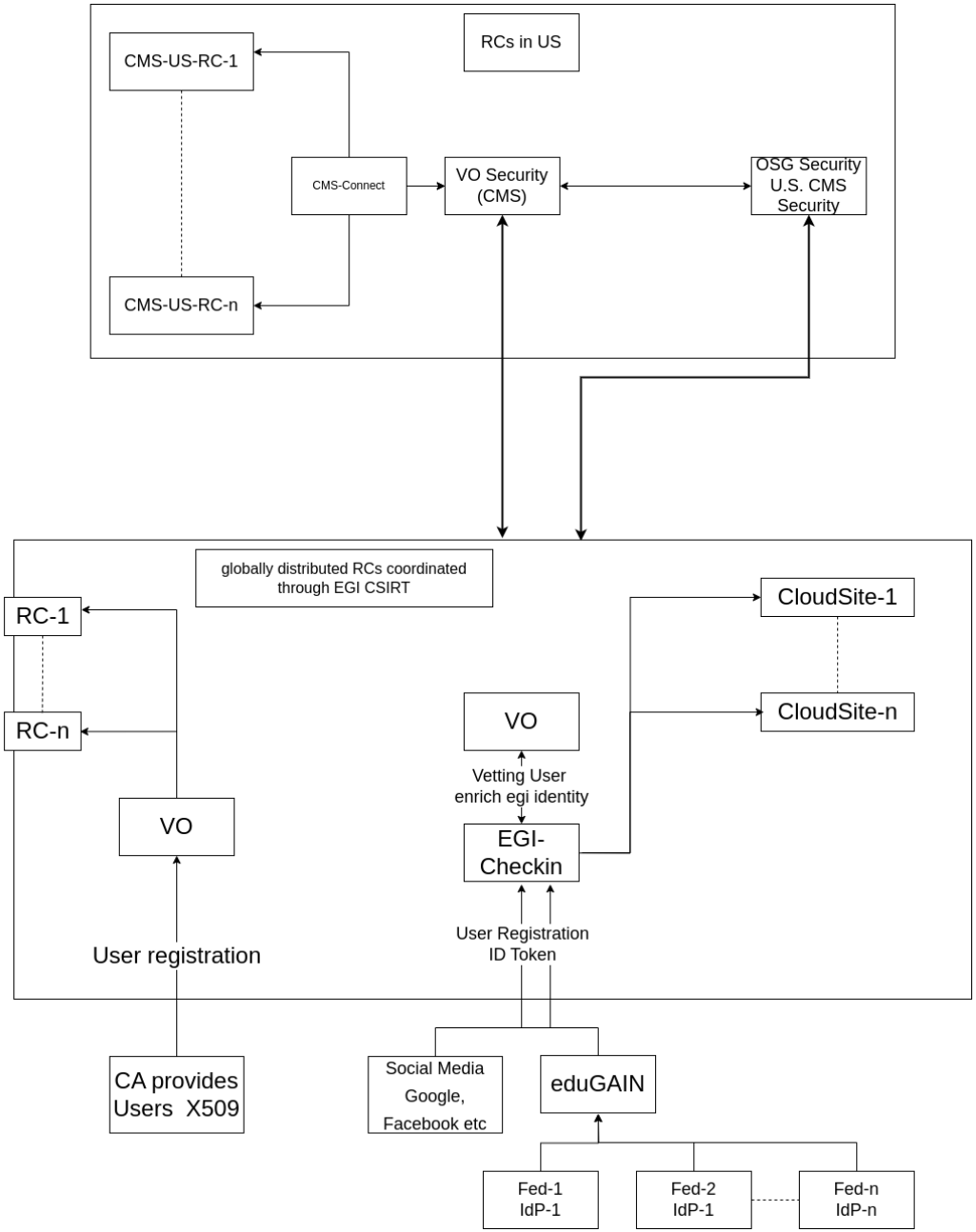
What to expect here . . .

- 3 Presentations, covering different aspects of the SSC.
- in total 45 minutes, we do the Q&A at the end.
- Get the presenters for more background info.

The Challenge, What, Hows

- Measure the overall Incident Response (IR) capabilities of our infrastructure and beyond.
- Set up a mock incident, let the involved teams do their thing (follow their procedures)
- Measure key aspects of IR: Communication Response Times, Containment activities: Stop malicious processes, suspend identities related to thee processes. Forensics (CTF, Check the training on Friday)
- Problems to solve: Which information is needed by who, and how can the information be retrieved.

The bigger picture



Scenario

- Get credentials, and use them for ...
- Deploy an attack infra (command and control system, ...)
- Create a Botnet on the infrastructures
- Does this seem unrealistic? Well, no.
- Next on the show, presentations by the other Chief Experts: how to get credentials, building the malware, then set the infra on fire, and finally how the blue team dealt with it.