EGI SSC Exercise Results - Q1 2023

Josh Drake
OSG Council Meeting
January 16, 2024

PATh PARTNERSHIP to ADVANCE THROUGHPUT COMPUTING

HT CENTER FOR HIGH THROUGHPUT COMPUTING

Full presentation - GDB Dec 2023

- Slides: https://indico.cern.ch/event/1225119/contributions/5675281/attachments/2771207/4828602/main.techex.pdf

- Video Capture: https://videos.cern.ch/record/2299441

Overview

- EGI conducted joint exercise involving EGI, WLCG, CMS/US-CMS and OSG in March 2023
- Exercise designed and run by EGI CSIRT (red team)
- Goal - evaluate detection, containment, mitigation, and forensics incident response capabilities at resource centers, and evaluation communication and cooperations between sites and organizations coordinating security activities (blue teams)

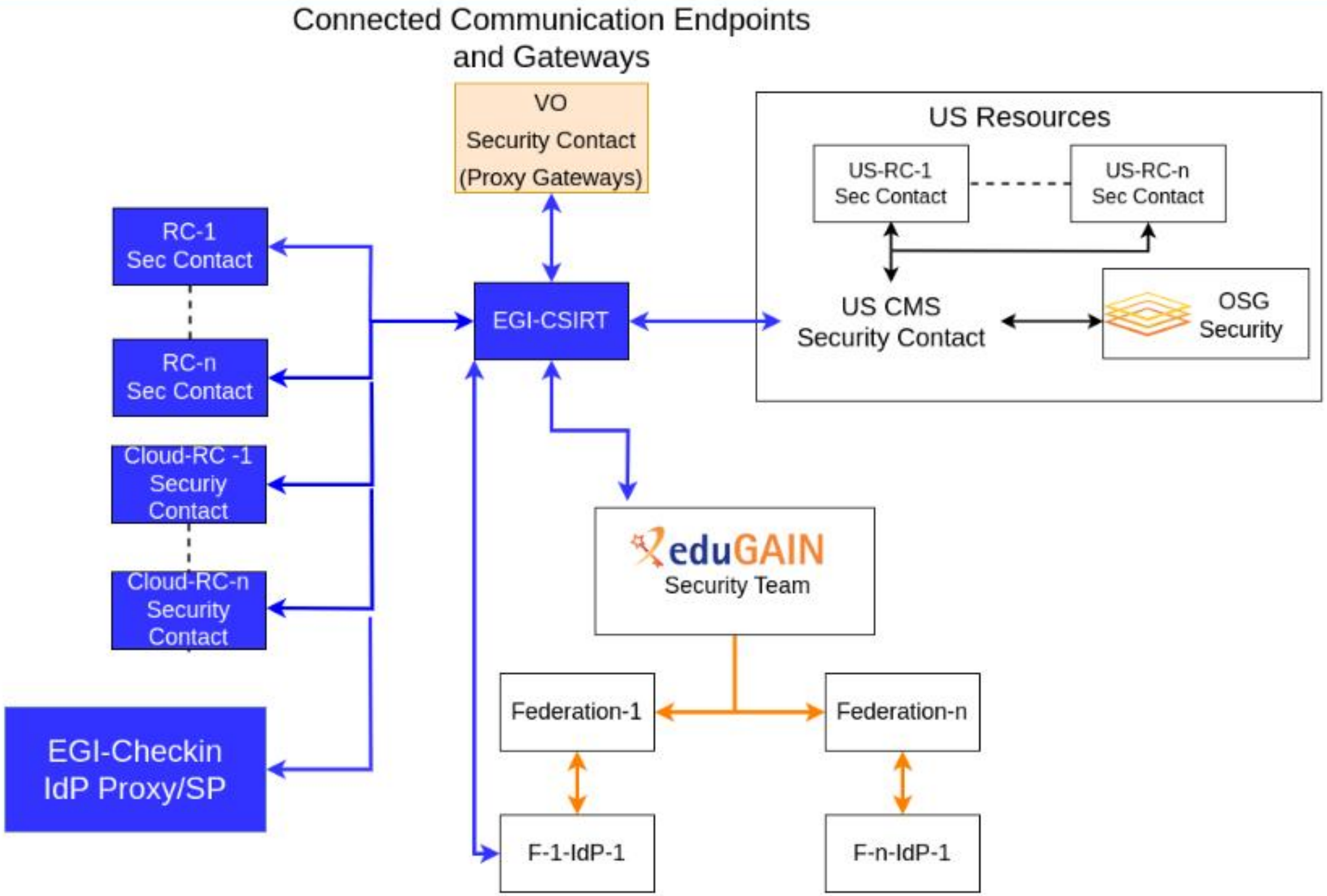
Methodology

- EGI Red Team obtained fraudulent or compromised x509 certs and computing accounts
- Deployed attack infrastructure at HTC and cloud based computing resources (CC, botnet, etc)
- Deployed malicious payloads at CMS/US-CMS sites on March 29
- Measured detection, reporting, and containment times for sites

OSG Participation

- One of four “blue teams” participating in the exercise
- No direct Open Science resources were targeted by exercise
- Role - coordinate response and threat sharing among affected US resources in coordination with US-CMS security
- Help collect data to enable response/forensics
- Primary US side contact was US-CMS Security Team

Communication Network



Findings

- 79 sites participated
- Most (40/79) did not respond to the exercise at all
- Out of the 38 participating sites
  - 34 responded inside of four hours
  - 4 within 16 hours
- All sites had revoked the access and ended malicious processes 12 hours - mostly as a result of fast action by IdP Federation

Findings (2)

- There is a significant delay between invalidating an IdP identity at the federation level and halting the VMs started by that identity
- Token lifetime is an issue, tokens are generally too long lived
- There is a need to duplicate CRL functionality for x509 be in Token based environments
- Accompanying CTF demonstrated high capabilities of teams at sites and received positive feedback

Lessons Learned (EGI)

- Need for up to date and verified security contacts before this exercise
- Blue teams at sites are largely understaffed
- Communications and Handoff of responsibilities between blue teams is not well defined, effectiveness is mixed
- Differences in operational environment and governance means suspensions processes used by EGI/WLCG not available to US-CMS/OSG
- The role/borders between security teams on US side is not clear, ownership and communication expectations for a given site are not well defined

Lessons Learned (OSG)

- Despite closer working ties, formal processes are still poorly defined or inaccurate
- Quickly sharing information across blue teams still challenging
- OSG's site security contacts lists are out of date (previously identified issue)
- No US-CMS sites or OS Pool/US-CMS sites contacted the OSG security team about the incident
- The eduGain CSIRT was very responsive and effective at suspending compromised identities at the federation level
- Willingness to work together on threat intelligence sharing and incident response is very high, but formal processes for sharing information and coordinating response are undefined, need an owner.