GMOC Procedure –Security Event, Vulnerability, and Attack

GMOC is responsible for receiving and responding to notices of security events on GENI. These notices range from critical active events to notices of vulnerabilities. GMOC will need to work with local GENI site administrators, Racks Teams (InstaGENI, ExoGENI), GPO and experimenter operations to resolve these events. We break these notices down to 2 types Active Events and Security Notices.

Active Event: GMOC receives email/phone call informing us a security event (DDOS Attack etc..) that is currently active on a GENI resource.

Security Notice: GMOC receives email/phone call informing GMOC of a confirmed or potential security vulnerability on a GENI resource.

Initial Information Gathering

In case of either event GMOC will need to create a ticket and record as much of the below information as possible.

- Initial reporters contact information. NOTE: Verify information in the GMOC DB.
    - Name
    - Organization
    - GENI Site Name
    - Phone Number
    - Email Address
- Type of Event
    - DDOS, Poodle vulnerability etc…
- What GENI resources are involved/affected.
    - GENI Site Name/Tool
    - Rack/Host
    - IP
    - Slice
- When did this start?
- Symptoms and Impact to GENI
- Criticality of Issue

Note: While GMOC is 24x7 GENI and its partners operate on normal business hours model. This means no anticipated after hours support or responses from other GENI members.

Active Security Events

Once the initial gathering of information is complete, follow the below process when responding to an Active Security Event. All steps and communication should be documented in the ticket.

- **During Business Hours**
    - ***GENI Team Handoff:*** Contact appropriate parties needed to resolve issue based upon initial information gathering. Please note the initiator should be CC'ed on all email communication

  - Local Site Admin
    - By Phone and Email
      - Phone and email are found in the GMOC DB
  - ExoGENI or InstaGENI Rack Team
    - InstaGENI: instageni-ops@flux.utah.edu
    - ExoGENI: exogeni-ops@renci.org
  - Experimenter ops List
    - gpo-expt-support@geni.net
  - Open GENI
    - gram-dev@bbn.com

- If no response in 2 hours Implement and create LLR Ticket.
  - Email those contacted above informing them the LLR procedure has been initiated.
  - If emergency stop is approved then inform those contacted that it was approved and implemented.
    - In the correspondence it should be noted that the resources will not be brought back online until the underlying security issue has been verified as resolved.
- Follow up with the parties initially contacted to insure issue has been resolved.
  - Update Ticket
  - Send Notification to the community
  - Determine if after action report is needed
  - Close ticket

- **After Business Hours**
  - Create LLR Ticket.
    - Email appropriate team informing them the LLR procedure has been initiated.
    - If emergency stop is approved then inform those contacted that it was approved and implemented.
      - In the correspondence it should be noted that the resources will not be brought back online until the underlying security issue has been verified as resolved.
  - ***GENI Team Handoff:*** Contact appropriate parties via email that needed to resolve issue. Please note the initiator should be CC'ed on all email communication
    - Local Site Admin
      - By Phone and Email
        - Phone and email are found in the GMOC DB
    - ExoGENI or InstaGENI Rack Team
      - InstaGENI: instageni-ops@flux.utah.edu
      - ExoGENI: exogeni-ops@renci.org
    - Experimenter ops List
      - gpo-expt-support@geni.net
    - Open GENI
      - gram-dev@bbn.com

- Follow up with the parties during next business day until the issue has been resolved.
    - Update Ticket
    - Send Notification to the community
    - Determine if after action report is needed
    - Close ticket