XSEDE SecOps Activities

Reporting, Meetings & Workshops

In addition to the regular reporting (e.g., quarterly & annual reports, updating risk registers, reporting project improvements), the XSEDE Security Office runs or is involved in several meetings and workshops. The XSO, which includes the two SecOps L3 managers, has regular planning calls, and leads several meetings, including a weekly incident response call with the XSEDE Trust Group, a biweekly call with the XSEDE Security Working Group, and a biweekly meeting between SysOps and SecOps. The XSO also attends the weekly Operations calls, quarterly meetings, and annual reviews as well as collaborates with national and international partners through workshops and calls, (e.g. the NSF Cybersecurity Summit, IGTFT/TAGPMA meetings, and WISE workshops).

Operational Services

Though most XSEDE Enterprise Services are run operated by SysOps, the SecOps team is responsible for the identity services that form the backbone of XSEDE’s trust fabric. These services include running an IGTFT accredited certificate authority, an OAuth service, and a Kerberos realm, as well as, providing individual host-based certificates and the set of trusted root certificates for XSEDE.

Regular Activities

In addition to the regular meetings, reporting and services managed by the SecOps team, it has several additional duties.

- **XSE audits:** Critical XSEDE Enterprise services (e.g., the User Portal, Single-Sign-On Hub, RT ticket system) are assessed by the security team against established security standards.
- **Incident Response:** The SecOps team is responsible for leading incident investigations, writing incident reports, and running incident response drills regularly.
- **Security Reviews:** The SecOps team with the XSEDE Security Working Group (XSWoG) performs security reviews of new services in coordination with XCI or other partners bringing new services to XSEDE (e.g., Globus Online)
- **Vulnerability Scanning:** SecOps regularly scans important XES and works with the SysOps team to remediate high priority vulnerabilities.
- **Policy Development:** The XSO, with assistance from other SecOps team, regularly updates a security risk assessment for XSEDE.
- **Administration of Security Services:**
  - XSEDE Certificate Authority
  - OAuth service
  - CILogon service
  - Kerberos service

SecOps Special Projects

In addition to these regular and on-going activities, the SecOps team has several special initiatives. As of October 2017, these include:

- **Federated Intel Sharing:** Volunteering SPs are deploying the Science DMZ security appliance (SDAIA) to share real time intelligence on attackers. This will begin by simply sharing the IPs of hosts blocked at participant organizations.
- **XSWoG Restructuring:** To make these meetings more efficient and to track tasks better, we are moving towards a JIRA Kan Ban board to track all the activities. Further, we are streamlining the meetings by moving XES vulnerability management to the new SecOps/SysOps coordination call. The new meeting format for this working group will start with new issues, move to RT ticket reviews, go over vulnerabilities discovered with allocatable resources, and end with a review and update of tickets in the Kan Ban board.

Non-SecOps Special Projects

In addition to the projects led by SecOps, there are often externally led projects in which the SecOps team participates. As of October 2017, these include:

- **XSEDE Data Sharing and Privacy:** XSEDE is looking for ways to more easily share its generated data with researchers. As part of this, the SecOps team has updated the XSEDE privacy and data sharing policy with a new draft for review, developed a document of XSEDE’s PII, and identified current risks with PII. As appropriate, the XSO will also recommend data that cannot be shared or must be sanitized.
- **Training Accounts:** The XSO has given recommendations and feedback on ways to improve the security of how training accounts are used within XSEDE.
- **XSEDE Multi-factor Authentication:** The SecOps team has always been a proponent for MFA within XSEDE and helped create requirements for the initial rollout. As XSEDE is exploring new MFA option, the XSO is also given recommendations and feedback.