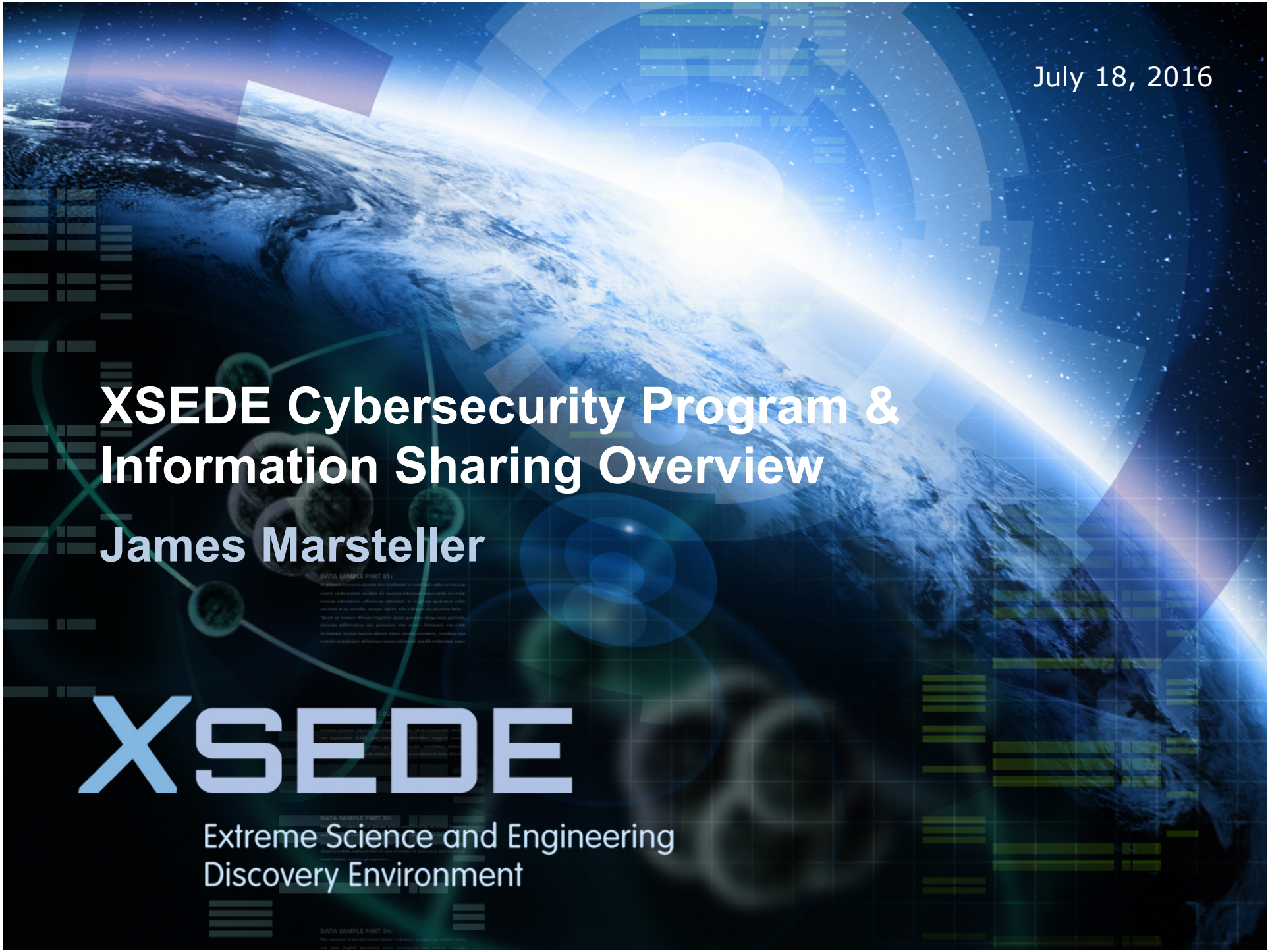

July 18, 2016
XSEDE Cybersecurity Program & Information Sharing Overview
James Marsteller
XSEDE
Extreme Science and Engineering Discovery Environment

# Agenda

- XSEDE Security Team Background
  - Goals/Mission
  - Structure
  - History
- Policies and Procedures
- Incident Repose Program

# Mission & Goals

- The primary mission of cybersecurity in XSEDE is to provide for the confidentiality, availability and integrity of all XD resources, services and data, and to promote cybersecurity education for all XD users and staff.
- **Goals include:** Provide security services that meet XSEDE distributed computing requirements by;
  - Performing a risk/threat analysis as input to security architecture and approach
  - Following best practices
  - Design, implementation and maintenance of cybersecurity in the XSEDE architecture
  - Fostering teamwork among XSEDE security staff
  - Integration of new security technologies, and procedures
  - Education, training, definition and implementation of best practices
  - Cooperation with XSEDE staff, Service Provider staff, and end XD users, supporting their job duties and scientific and research missions.

# XD Security Organization

- **XSEDE Security Office (XSO)**
  - Oversee XD security activities, & provide a single point of contact for both internal and external security.
  - Responsible for operational computer security for XSEDE, security advancements, and coordination with other XSEDE teams.
- **XSEDE Security Working Group (XSWoG)**
  - Service Provider (SP) Security Leads (~10)
  - Operational security, incident response, policy/procedure development, security design reviews
- **Cybersecurity trust group**
  - SP leads + non-XSEDE security relationships (CERN, LIGO, NERSC)

# XSEDE Security Team History

- Formed in January 2004 (then the Teragrid project)
- FBI Case 216 (Stakkato Incidents)
  - US Military
  - NASA
  - White Sands Missile Range
  - CalTech, SDSC & other .edus
  - CISCO (Stole IOS source code)

# XSEDE Security Policies & Guidelines

- Security WG Charter
- Acceptable Use Policy
- XSEDE Security Playbook
- Security WG SP guide and FAQ
- Central Baseline Security Standards
- Science Gateway Security Policy
- Level 1 SP Security Agreement
- Privacy Policy

# Early Lesson Learned

Rapid, Secure, Coordinated Response and Information Sharing is Critical!

# XSEDE Incident Response (IR)

- Weekly "Response" Calls
- 24 Hour Security "hotline"
- Incident Mailing Lists
- Encrypted Communications
- Coordinated Evidence Gathering
- IR Tracking on secure wiki

# XSEDE Incident Response (IR)

- Weekly IR Calls
  - Value: grandfathered now defunct SPs as participants (Cybersecurity trust group)
  - 5 to 45 minutes in length
  - ‘Closed’ Participant List
  - Share Latest Attack Vectors
  - Honeypots, Non-XSEDE News
  - Vulnerability assessment
  - Update On Investigations

# XSEDE Incident Response (IR)

- "Hotline"
  - 24/7 Conference #
  - Any Site Can Initiate
  - Only Known To Response Personnel
  - Participants ID Verified
  - 800 Number & International Access

# XSEDE Incident Response (IR)

- Response Playbook
  - Who/How To Contact Methodology
    - Initial Responders
    - Secondary Responders
    - Help Desk Staff
  - How to Respond to Event
  - Reporting Guidelines:  Press, Privacy, Funding sources

# XSEDE Incident Response (IR)

- Expect to provide the following information as available and relevant:
  - Hosts affected at your site; User accounts affected; and Source of compromise (remote hosts)
  - Nature of compromise (e.g. remote vulnerability, local vulnerability, etc.)
  - Signatures of compromise (log messages, files installed/modified, etc.)
  - Other XSEDE sites, which may have been touched by intruders
  - Completed Compromised User Account Questionnaire

# XSEDE Incident Response (IR)

- **Compromised Account Questionnaire**
  - Do you use the password of the account at other TG sites or other general accounts (gmail, Amazon, Paypal, Ebay)?
  - What was the time of your last known login?  Where was it from?
  - From what locations do you usually login (hostnames/IP)?
  - Which sites/machines have you used?
  - Which do you expect to use?
  - What locations (hosts) can we expect to you to login from?

# XSEDE Incident Response (IR)

- Communications & Information Sharing
  - Mailing lists
    - Ops-Security WG List
    - Incident-Announce: Announce weekly IR Calls/Notes
  - Security Contact List
    - IR, General Security, NOC, Phone, email and pagers
  - Jabber Chat Service

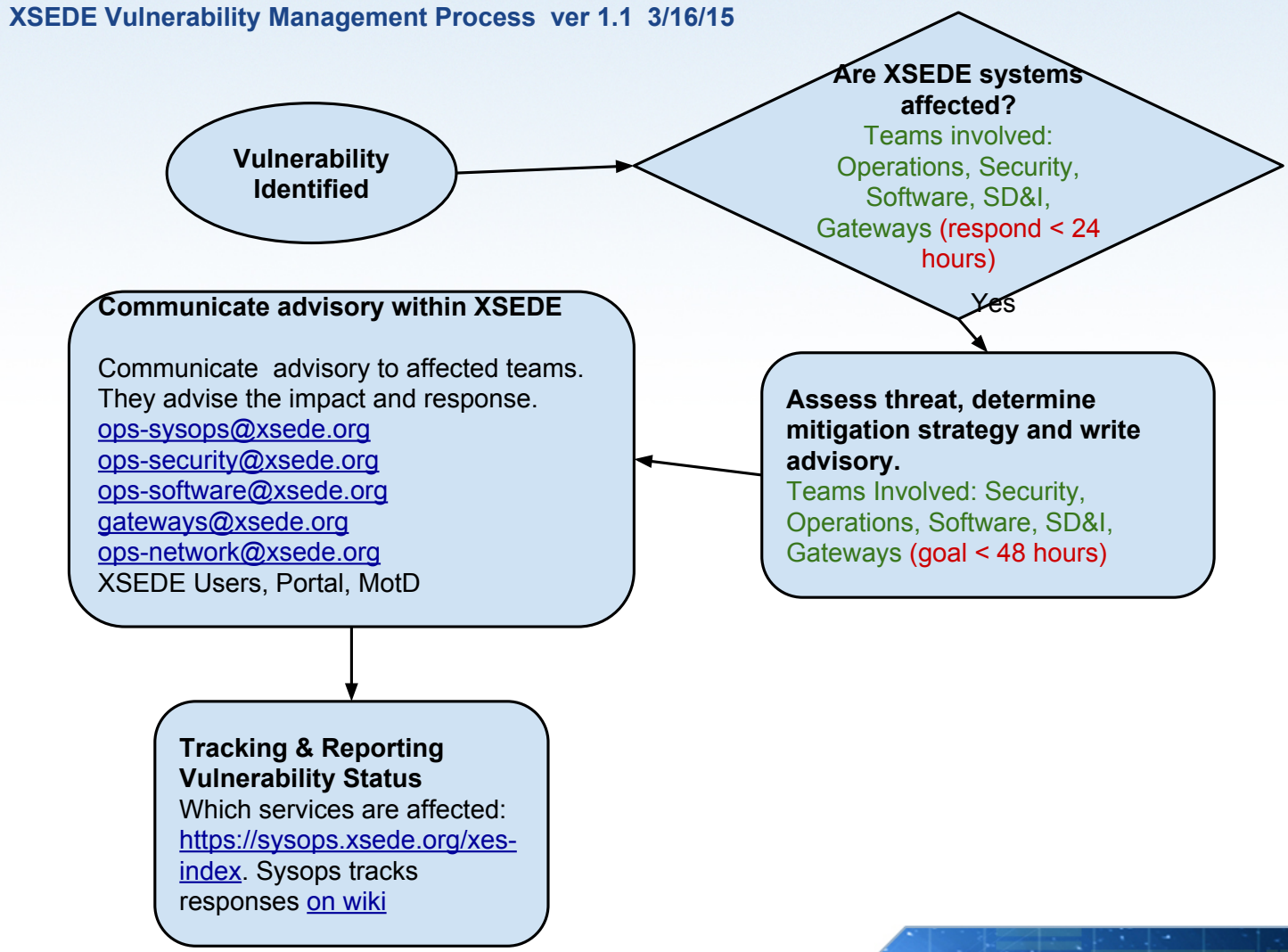
# XSEDE Incident Response (IR)

- Encrypted Communications
  - PGP Key Signing
  - Symmetric Encryption (shared password) for Email Communications
  - Jabber service with IR Chatroom
  - Secure Wiki To Archive Critical Information
  - Encrypted Communications Are VERY IMPORTANT!

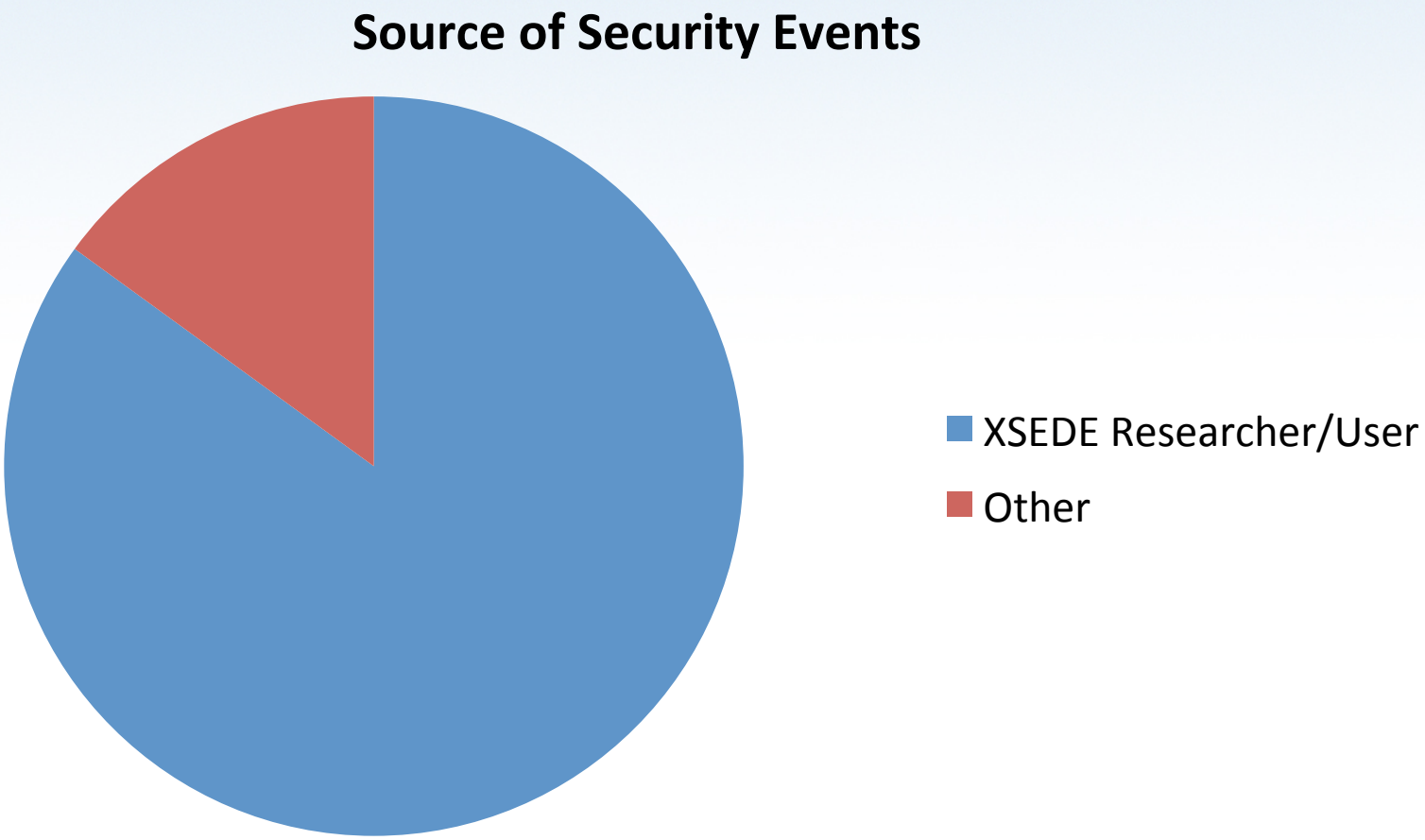
# XSEDE Vulnerability Management

- Security team reviews, assesses impact and mitigation strategy.
- Communicates advisory to XSEDE teams (software, networking,,,)
- Teams report their Reponses
- Tracking for high impact vulnerabilities

# XSEDE Vulnerability Management



# Attack vectors



# Defense Toolbox

- SP - Monitoring, Detection, and Incident response coordination
- SP - 2FA for privileged access
- SP - participation in REN-ISAC
- XSEDE Level - Vulnerability auditing/scanning
- XSEDE Level – Information security training for new users

# Training Overview

- Security Awareness
- You Are The Target
- Social Engineering
- Email and Instant Messaging
- Using Your Browser Safely
- Passwords
- Encryption/Data Protection
- Mobile Devices
- Protect Your Computer
- Wi-Fi Security
- Social Networking
- Reporting a Security Incident

# Future XSEDE Security Projects

- Federated Intelligence Sharing
- Compromised/bad SSH Key fingerprint directory

# Contact Info

- https://www.xsede.org/security
- My Email:  jam@psc.edu