



Open Science Grid

# PI Talk

Mike Stanfield

OSG Security Team

Center for Applied Cybersecurity Research

Indiana University

April 19th, 2021

## Who is actively working on the project from the group and what are they doing?

---

- Mike Stanfield
  - Information Security Officer
- Zalak Shah
  - Security Analyst
- Josh Drake
  - Security Analyst
- Adrian Crenshaw
  - Security Analyst

# What are contributions of those individuals in your group to the various area(s), i.e. AS, IA, DOMA, SSL, SSC, OSG-LHC, MGMT

---

- As a group we support OSG-LHC, providing operational security support.
  - Vulnerability announcements
  - Vulnerability scanning
  - Application penetration testing
  - Security exercises
  - Architecture review
  - Policy

## What specific collaborations has the group made with other groups within IRIS-HEP?

---

- We are working with the SLATE team in SSL to provide guidance on security policy and container security.
  - This particular project has a potentially broad impact on the WLCG, so OSG Security collaboration is critical.



## What specific collaborations has the group made with other groups or individuals external to IRIS-HEP?

---

- EGI CSIRT and SVG
- U.S. ATLAS and U.S. CMS
- BNL and FNAL
  - coordinating incident response, vulnerability announcements and threat intelligence
  - joint exercises
  - info sharing from external meetings, working group memberships, etc.

# Which contributions has the group made to the "Intellectual Hub" aspect of IRIS-HEP? (Including community building activities, training, outreach and broader impact.)

---

- WLCG Federated Operation Security Working Group
- Cross-membership with EGI CSIRT
- Joint EGI/OSG incident response/communication coordination exercise.

Please list any  
papers/presentations/software-repositories  
connected to the above.

---

- OSG-EGI security drill report (March 2020 GDB meeting)
  - <https://indico.cern.ch/event/813745/#7-osg-egi-security-drill-repor>

## How is your project managed? How is progress measured? How are risks identified and mitigated?

---

- Managed through OSG-LHC:
  - weekly Security team meetings
  - milestones tracked in JIRA
  - operational tickets in JIRA, customer tickets in FreshDesk
- Progress measurements are fuzzy
  - milestone completion
  - potential for maturity metrics?



## Are metrics aligned with the project? Do metrics accurately reflect the progress, success or impact of the project?

---

- Realigned metrics in Q12020 and again in Q12021 to better fit reality
  - old metric: number of tickets resolved
  - new: number of incidents per quarter, number of hosts scanned for vulnerabilities, number of vulnerabilities detected that require remediation
- New metrics also include clear thresholds for action from the OSG Executive Team