GridPP

UK Computing for Particle Physics

Future GridPP Security

David Crooks (STFC UKRI)

GridPP42 25 April 2019

WLCG

Worldwide LHC Computing Grid

egi

WISE COMMUNITY

EOSC-hub

Post SSC

- Ongoing evaluation of SSC results
- Can already make some plans
- Present here for discussion and hopefully agree way forward

Site requirements

- Some things made clear (which we knew anyway…)
- Sites are typically staffing limited, regardless of size of site
- But, most especially where we have limited FTEs

Site requirements

- Security asks things of sites
- Both via policy, but in particular as a healthy community
- What do we **need** from sites?

Site requirements

- Components involved with incident response

- Communication
- User suspension
- Containment
- Tracking activity
- Forensics
- Reinstall
- Lessons learned and final report

Site requirements

- Components involved with incident response

- **Communication**
- **User suspension**
- Containment
- Tracking activity
- Forensics
- Reinstall
- Lessons learned and final report

Site requirements

- From an operational security standpoint, we need to be clear about what we ask sites for
- If we **require** action, need to be clear about what this is.

- Base requirements

- **Respond to emails**
- **Ensure that central suspension system is in place and effective**

How do we achieve this?

- Feedback from SSC
  - I’ve spoken to several people already
  - Seek to talk to all sites in person (either here or by coming for a visit)
  - If I haven’t, please get in touch as I want to give everyone a chance to give feedback!

How do we achieve this?

- Communications
  - Security-discussion was extremely useful
  - Other channels (mattermost team?)

How do we achieve this?

- Documentation
  - Started a round of revisions with Job Tracing page
  - This needs additions (pilot jobs!)
  - Continue to build this out, based on…

GridPP
UK Computing for Particle Physics

How do we achieve this?

- Training
  - HEPSYSMAN Security Day
  - Individual site training?

How do we achieve this?

- Test framework
  - Break components of incident response into different parts
  - Communication chain
  - Tracking activity
  - Test these individually, on a per site basis
  - Written component?
  - Tabletop exercises?

How do we achieve this?

- GridPP security tools
  - Proposing to use SCD Cloud to host a set of tools/test scripts/etc.
  - Allow access for development by Security Team
  - Common home/ACLs/development area
  - Start with simple tests, but have common area for progress

How do we achieve this?

- End result

- Consider we may have SSC every ~2 years
- Develop plan of GridPP documentation, training and testing in preparation
- SSC (for us) should be execution of well understood techniques

HEPSYSMAN Security Day

- First iteration of training, following hiatus last year
- Morning:
  - Review of basic procedures – what we ask of sites
  - Technical review of SSC lessons learned
  - Security tools – following Technical Meeting earlier in the year
- Afternoon:
  - Forensics training
  - Daniel Kouril (EGI CSIRT/CESNET)
  - Hoping to have guided analysis of SSC payload

EGI Conference

- Two security sessions + talks
- SSC Overview
- SSC Forensics training

Next 6 months

- Run some test jobs at sites to practice tracing jobs
- Start with most common submission methods
  - And those particular to us (GridPP DIRAC)
- Much of this experience we have already – this is an opportunity to practice
  - SSC feedback – effectively performing gap analysis of procedural requirements
  - Ultimately best done through experience

Security Team

- Plan for security team to help with testing and training
- Focus the mandate of the team following our recent experience
- Grow our numbers a little

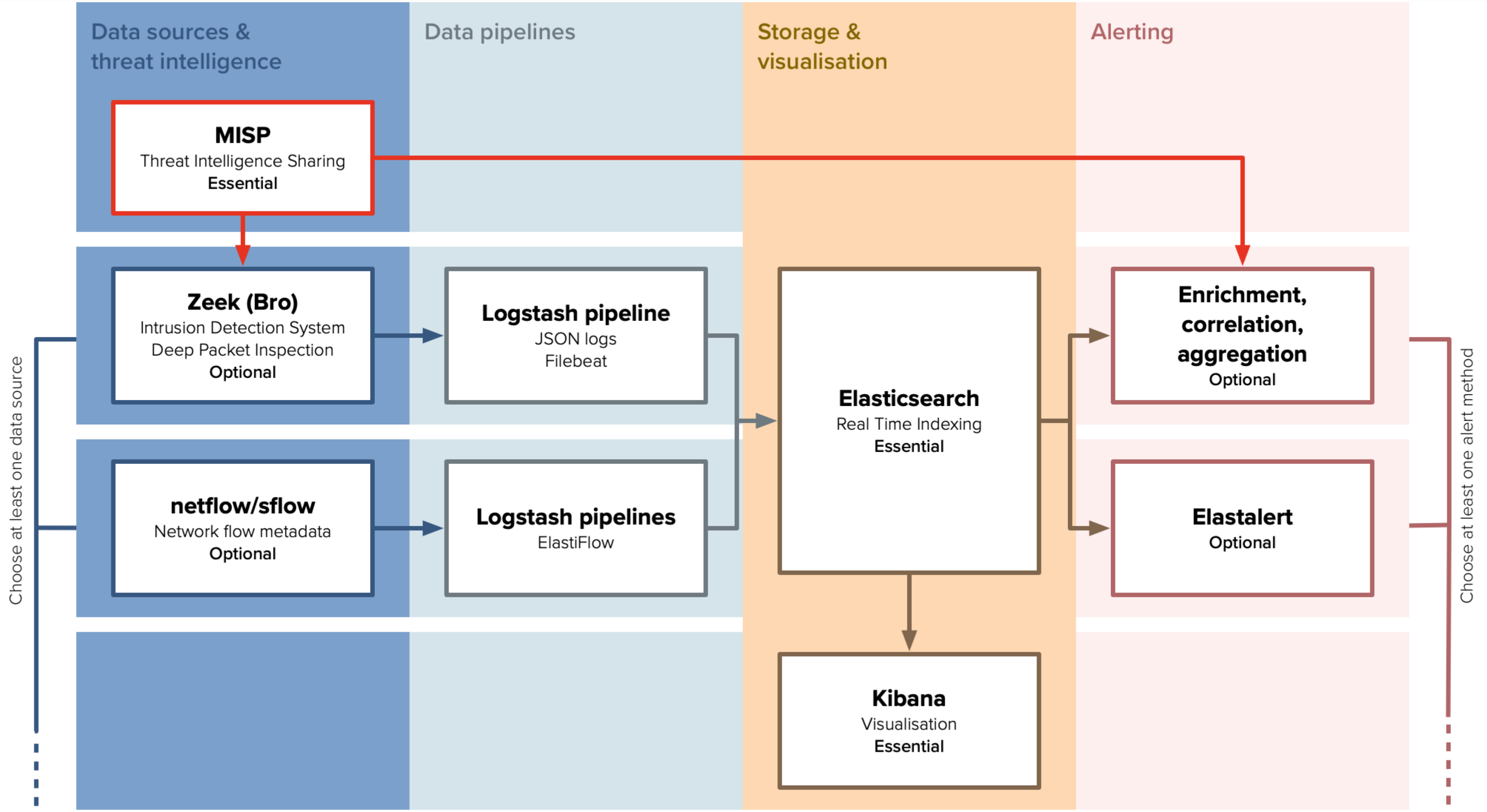
Wider topics

Security Operations

- SOC Workshop in February
  - Co-located with policy meeting and EGI CSIRT F2F
  - Good attendance
  - SOC WG Initial Model

- Projects ongoing/starting up at Nikhef and on SCD Cloud to test deployment
- Identify MISP as a priority to enable access to intelligence

Security Operations



Data sources & threat intelligence

Data pipelines

Storage & visualisation

Alerting

MISP
Threat Intelligence Sharing
Essential

Zeek (Bro)
Intrusion Detection System
Deep Packet Inspection
Optional

Logstash pipeline
JSON logs
Filebeat

netflow/sflow
Network flow metadata
Optional

Logstash pipelines
ElastiFlow

Elasticsearch
Real Time Indexing
Essential

Kibana
Visualisation
Essential

Enrichment, correlation, aggregation
Optional

Elastalert
Optional

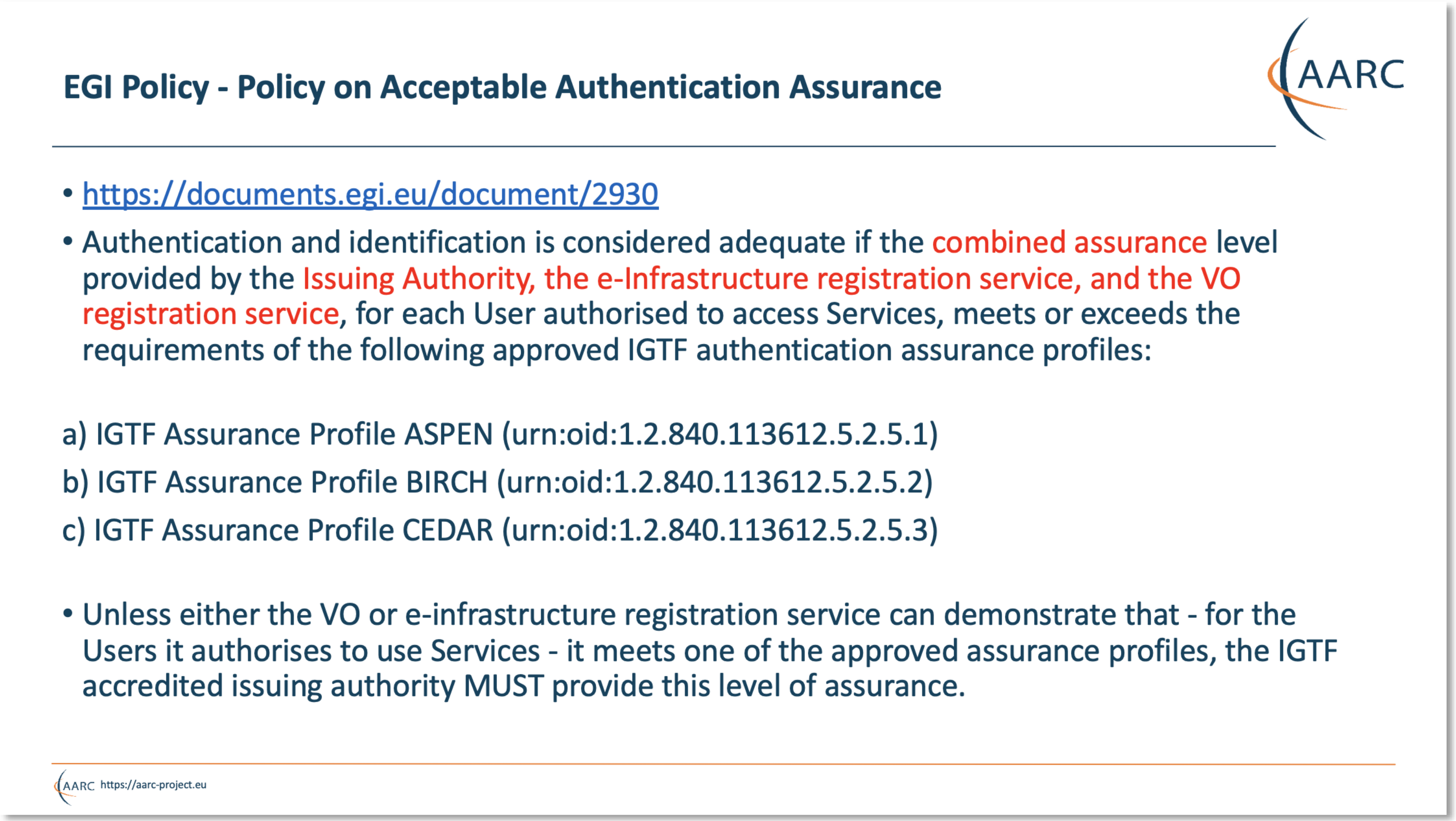
Choose at least one data source

Choose at least one alert method

Security Operations

- Threat Intelligence
- Making this available to share IoCs related to WLCG related incidents
- WLCG CERN MISP
  - TLP: AMBER as well as TLP: GREEN and WHITE
- SIRTFI IdPs
  - https://technical.edugain.org/entities (within eduGAIN)
  - If your site is not on the list, recommend following up with your institutional provider
  - 4 GridPP sites
  - 557 entities across 28 federations
- Used PocketSOC demonstrator to ingest traffic from malware analysis
  - Trigger alerts using real MISP event

Combined Assurance



EGI Policy - Policy on Acceptable Authentication Assurance

AARC

- https://documents.egi.eu/document/2930
- Authentication and identification is considered adequate if the combined assurance level provided by the Issuing Authority, the e-Infrastructure registration service, and the VO registration service, for each User authorised to access Services, meets or exceeds the requirements of the following approved IGTF authentication assurance profiles:

a) IGTF Assurance Profile ASPEN (urn:oid:1.2.840.113612.5.2.5.1)

b) IGTF Assurance Profile BIRCH (urn:oid:1.2.840.113612.5.2.5.2)

c) IGTF Assurance Profile CEDAR (urn:oid:1.2.840.113612.5.2.5.3)

- Unless either the VO or e-infrastructure registration service can demonstrate that - for the Users it authorises to use Services - it meets one of the approved assurance profiles, the IGTF accredited issuing authority MUST provide this level of assurance.

AARC https://aarc-project.eu

Combined assurance

- Impact for
  - LIGO
  - SKA

WISE

- Wise Information Security for collaborating eInfrastructures
  - https://wise-community.org

- Active Working Groups:
  - Updating the SCI framework (SCI-WG)
  - Risk Assessment WISE (RAW-WG)

- Working Groups being created:
  - Incident Response & Threat Intelligence Working Group (IRTI-WG)
  - Security Communications Challenge Coordination Working Group (SCCC-WG)
  - Security for High Speed Transmissions Working Group (S4HST-WG)

SIG-ISM/WISE meeting, Lithuania

- Recent joint GEANT SIG-ISM/WISE meeting in Kaunas, Lithuania
  - 16-18 April 2019
  - Linda Cornwall and David Crooks attended
- Joint discussions on areas of shared interest
  - Coordination of security communications challenges
  - Shared interest in SOC development – GEANT security working group task on Security Operations Centres
  - Risk Assessment

IRIS

- Proposal submitted for trust framework and incident response cooperation framework for IRIS
- Presenting at upcoming TWG
- Dave Kelsey, Ian Neilson and myself

Conclusions

- SSC was invaluable
  - Highlights needs for sites and community
  - Gives context to existing plans

- Wider collaboration
  - Security necessarily exists as a collaborative effort across many communities
  - Leading and participating in efforts across infrastructures
  - Sharing intelligence within appropriate groups is key element