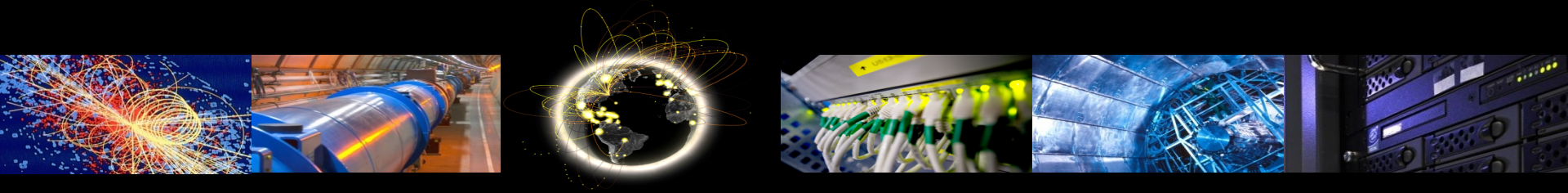
WLCG SOC WG update

WLCG Security Operations Center Working Group

David Crooks, Liviu Vâlsan



WLCG Worldwide LHC Computing Grid

GDB December 2019

CERN

Overview

- Update on October SOC Workshop
- Threat Intelligence and operational security
- Deployment options
- Next steps and summary

October SOC Workshop

- Most recent WLCG SOC WG Workshop took place in Nikhef, 21-23 October
  - Following HEPiX (which also included an update on the WG for that audience)
- Attendees included
  - WLCG sites, NRENs, GÉANT, EGI CSIRT

October SOC Workshop

- Status talks
- Access to MISP threat intelligence
- Mock incident (proof of workflow)
- Operational use of threat intelligence

Status updates

- STFC and Nikhef over the summer have deployed prototype SOCs
  - Nikhef: Zeek data source (OpenPOWER8)
  - STFC Cloud: sFlow from subset of hypervisors

- Update from GÉANT on their SOC related activities
  - Good alignment at threat intelligence level

- NetBASILISK
  - Inform the design of advanced network security devices for universities
  - Scale to accommodate the network traffic requirements of data intensive science

Mock incident

- Key test of SOC workflow
- Use EGI CSIRT SSC framework to simulate botnet involving STFC and CERN
- Trigger “malicious” activity at CERN
- Track using CERN SOC, generate MISP event
- Check propagation of MISP event to STFC
- Trigger same activity at STFC and check for alerts
  - *Successful test!*

Threat intelligence

- So far have discussed technology stack
  - Built a reference design
  - Initial deployments
  - Technology test of workflow

- What about threat intelligence itself?

Threat intelligence

- Important to have highly focused, relevant intelligence
  - Guidelines on what types of indicators to include
  - As specific as possible, *including context*

- What process do we use to sync intelligence between sites?
  - Focus on CERN instance as central hub
  - Access to other sites via separate MISP instances or direct API access
    - Anticipate many sites would use direct access
    - Explore tiered approach using UK instance (in development at STFC): c.f. Argus

Best practices

- Lots of discussion at the recent SOC Workshop
  - How best to make use of threat intelligence shared via central MISP instance hosted at CERN
  - Including WLCG and other scientific communities

- How does a site gain access to intelligence?
- What is expected of them?
  - Code of conduct
  - For example: respect TLP
- Maintaining high level of trust between participants sharing information is paramount

Threat intelligence & operational security

- Lead to clarification of role of WG
  - Including discussions at CHEP

- Draw a distinction between
  - the technologies, infrastructure and best practice used to share threat intelligence (focus of WG)
  - the threat intelligence itself and actual sharing of information in the course of operational security

Security Operations

- The CERN MISP instance is aimed at WLCG sites
  - Including campus/institution teams for those sites
- For other communities, please contact
  - wlcg-security-officer@cern.ch
- CERN instance designed to be open
  - **But** governed by strict rules of access to increase trust

Security Operations

- Document on guidelines for access to central instance hosted at CERN to be prepared by Romain/Liviu

- Practically, access to the CERN MISP instance is then controlled using CERN SSO
  - Federated access (EduGAIN+SIRTFI, preferred)
  - CERN account

Deployment options

- How might we suggest proceeding with a wider roll out of this capability?
- Current direction is towards encouraging participation particularly within Tier-1s
- Envisage a focus by the WG on assisting individual sites with deployment
  - Any volunteers?

Next steps

- Consideration of usage models at different sites (Tier-1s vs Tier-2s, for example)
  - Staffing implications
  - Additional components
- Continued work on existing deployments
  - And hopefully adding more participants!

Summary

- Progress made on adding initial capability to more sites
- During recent workshop, demonstrated SOC workflow
  - Important milestone
- Clarification of role of WG
  - Moving forward with how sites from different communities can access threat intelligence

Contact details

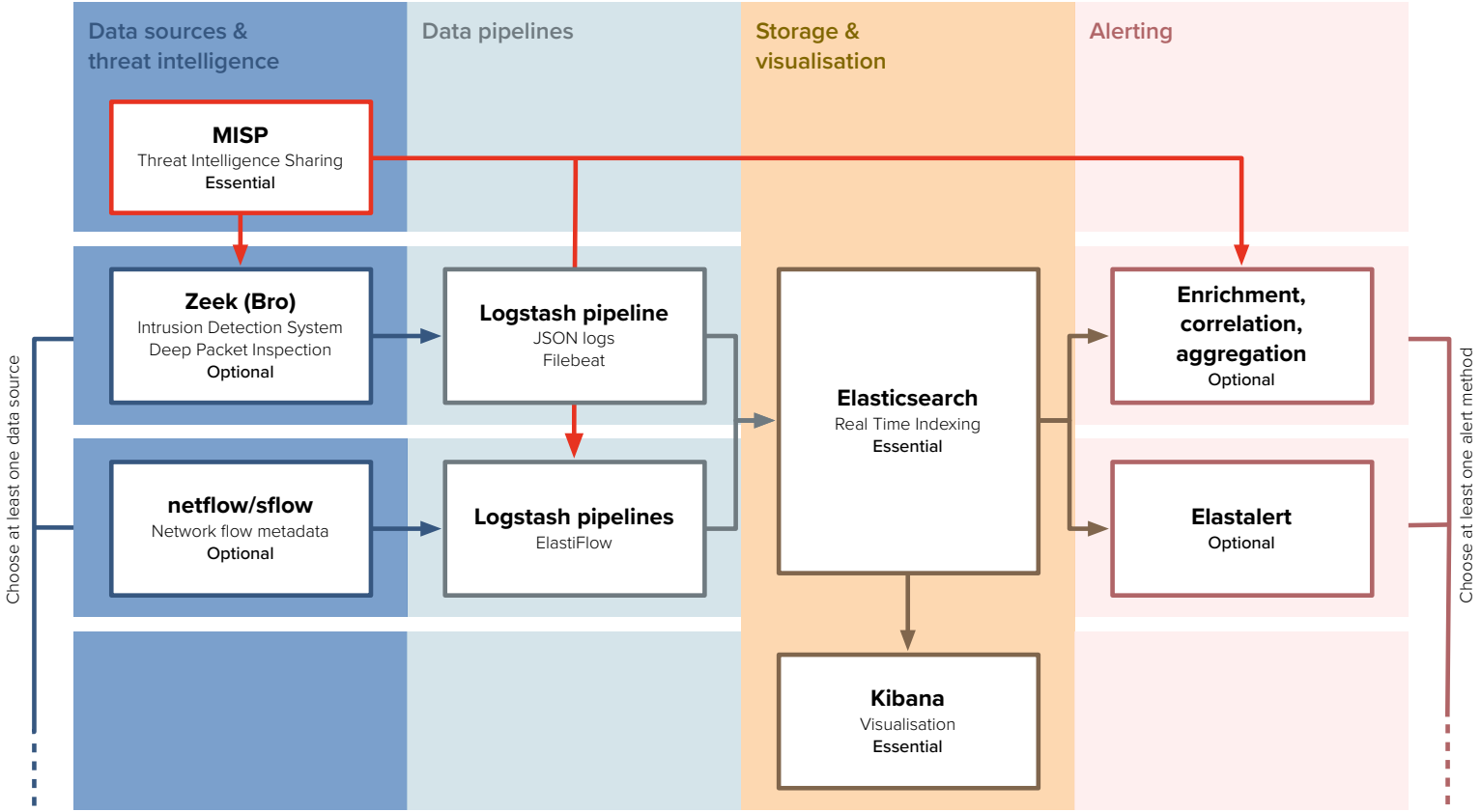
- Website
  - wlcg-soc-wg.web.cern.ch
- Documentation (recently updated with new format)
  - wlcg-soc-wg-doc.web.cern.ch
- Mailing list
  - wlcg-soc-wg@cern.ch

- David Crooks (david.crooks@cern.ch)
- Liviu Vâlsan (liviu.valsan@cern.ch)

- Access to CERN MISP
  - wlcg-security-officer@cern.ch

Backup slides

Technology stack: Initial Model



Technology stack: initial model

Stage	Component	Notes
Threat intelligence	MISP	Cornerstone of model; focused around central MISP instance hosted at CERN
Data sources	Zeek	Highly detailed but requires dedicated hardware
	Netflow	Readily available at many sites but offers less information than Zeek
Data pipelines	Logstash + Filebeat + JSON logs (e.g. Zeek)	Basic pipeline provided by WG
	Logstash + Elastiflow (Netflow)	Dedicated pipeline for netflow/sflow
Storage and Visualisation	Elasticsearch	Share deployment configs within group
	Kibana	Share dashboard processes
Alerting	Correlation scripts	Generalised version of CERN scripts
	Elastalert	Rule based alerts; share typical configs

Code of conduct: TLP

LEVEL	DEFINITION
RED	Not for disclosure, restricted to participants only
AMBER	Limited disclosure, restricted to participants' organizations
GREEN	Limited disclosure, restricted to the community
WHITE	Disclosure is not limited