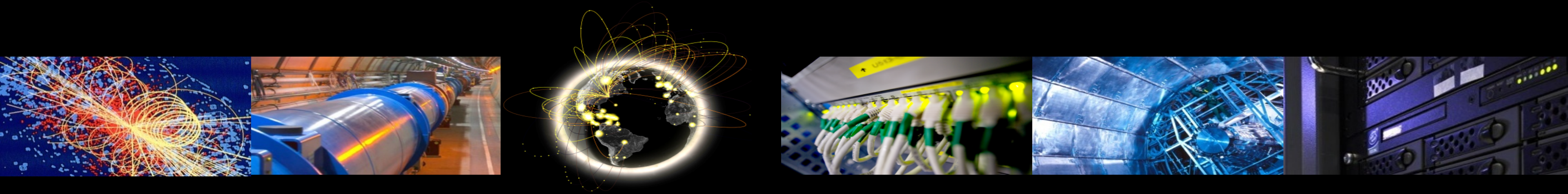
WLCG SOC WG

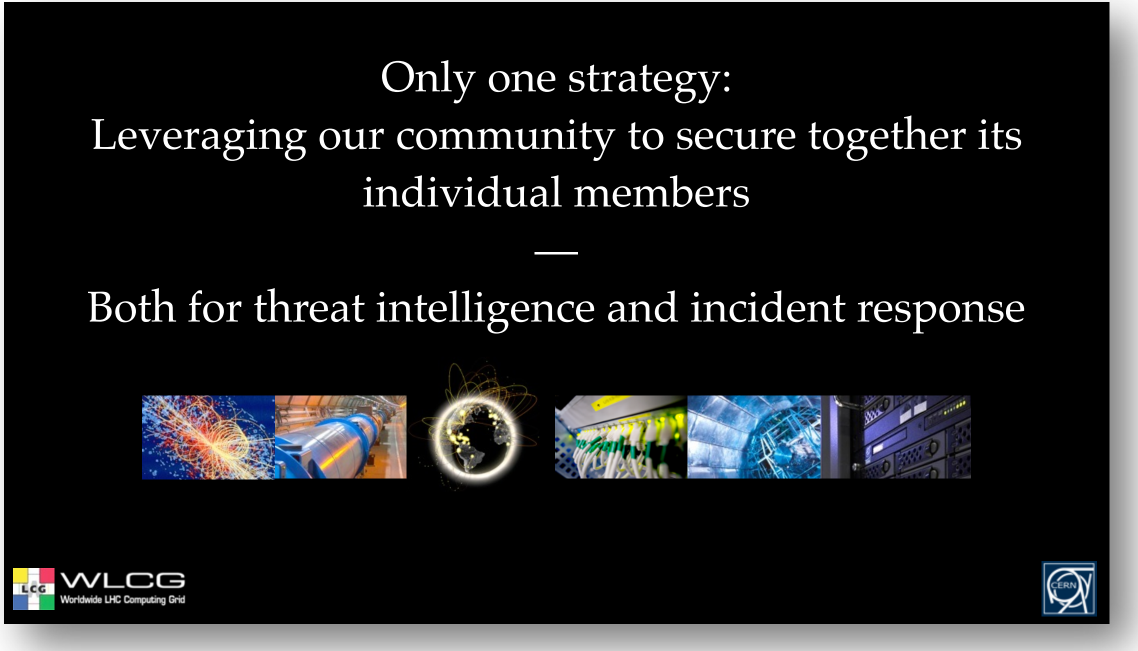
WLCG Security Operations Center Working Group

David Crooks, Liviu Vâlsan



SIG-ISM/WISE October 2020

Landscape



Only one strategy:
Leveraging our community to secure together its individual members

—

Both for threat intelligence and incident response

Romain Wartel

Computing for High Energy Physics 2019, Adelaide, Australia, November 2019

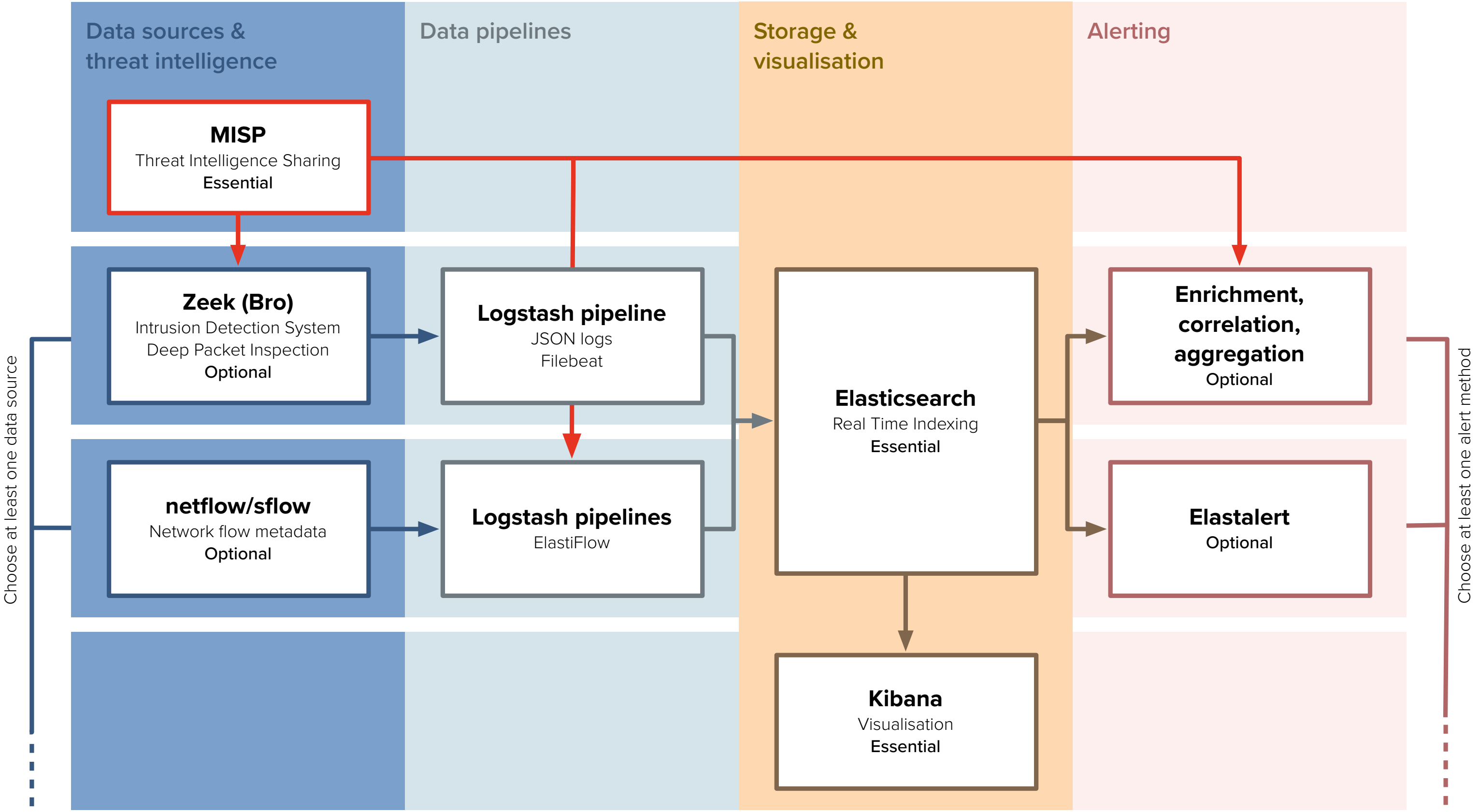
Security Operations Centres

- Allowing WLCG sites to digest and make active use of threat intelligence is a cornerstone of the WLCG security strategy
- The WLCG Security Operations Centre WG was established to enable the deployment of security tools to enable this
  - But also including members from the wider academic research community
- The working group is mandated to create reference designs to allow sites to
  - Ingest security monitoring data
  - Enrich, store and visualize this security data
  - Alert based on matches between the stored data and threat intelligence
    - Indicators of Compromise or IoCs

Areas of work

- Technology stack needed to actively use threat intelligence
- Integrations with existing tools
- *Not* in scope is operational use of threat intelligence
  - Existing operational security teams

Technology stack: Initial Model



SIG-ISM/WISE October 2020

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

CERN MISP

- CERN is currently operating 5 different instances:
  - Main CERN instance (~2.3 M IoCs)
  - Academic (Worldwide LHC Computing Grid (WLCG)) central MISP instance (~1.2 M IoCs)
  - Development MISP instance used for MISP development (CERN is an active contributor) and for validating new MISP releases
  - Two community specific MISP instances
- CERN is currently actively sharing threat intelligence with ~570 peer organisations

Academic MISP instance

- Hub and spoke intelligence sharing structure based around instance hosted at CERN
  - Benefit from CERN trust relationships and experience
- Mostly TLP:GREEN and TLP:WHITE
  - Information that is limited to the community or public
- TLP:AMBER events produced by CERN
  - Information that should only be shared with trusted security contacts
  - Important to allow sharing of intelligence safely about ongoing incidents
- Rules of participation document has been prepared for this service

Academic MISP instance

- Access to the Academic MISP instance governed by a Threat Intelligence Sharing Agreement
  - Rules of engagement
  - Use of the threat intelligence shared using this instance

- Information usage policy
  - Threat intel exclusively for the benefit of the trusted parties
  - Solely for the purpose of detecting, containing, mitigating and resolving security attacks

Access to Threat Intelligence

- Commitments
  - Follow and obey the TLP guidelines and sharing restrictions
  - Follow and obey the SCIv2 trust framework assertions IR1-4
  - Follow and obey the information usage policy
  - Share back information whenever you believe it may be beneficial to a trusted party and are in a position to do so

Threat intelligence & operational security

- Clarification of role of WG
- 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

Recent developments

- STFC continuing to work on Cloud SOC using sflow from cloud routers
- Plans in place to deploy prototype Zeek instance
  - Somewhat delayed by COVID-19
- Integrate threat intelligence with STFC Information Security
- Nikhef revisiting prototype Zeek deployment
- In contact with Triumf who have a project to deploy Zeek
- Discussions ongoing to integrate our threat intelligence with Jisc MISP

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

Contact details

- Website
  - wlcg-soc-wg.web.cern.ch
- Documentation
  - wlcg-soc-wg-doc.web.cern.ch
- Egroup
  - wlcg-soc-wg@cern.ch

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

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