

# Security Operations Centers WG

---

David Crooks and Liviu Vâlsan

[wlcg-soc-wg@cern.ch](mailto:wlcg-soc-wg@cern.ch)

- A need for external observability of systems & networks
- Increasing amount of security monitoring data being produced
- Identify tools available to WLCG sites of different sizes and provide appropriate guidance
- Leverage data analytics and Big Data frameworks used within our communities to provide security alerting, traceability and forensics information

- Identify data that SOC's can / should provide
  - Both in terms of sources from which the SOC ingests data as well as necessary outputs
- Identify necessary components of a SOC for typical WLCG sites of different sizes
  - Recognising that local needs will be likely to vary
- Reference designs for SOC's of different sizes which could include installation guidance or appliances

# Scope

- Identify key stakeholders to be considered in the deployment of a typical SOC, including but not be limited to:
  - Local sysadmins
  - Local security teams
  - Campus security teams
  - NGI security teams/officers
  - VO Security teams
- Data protection / privacy and information sharing policies
- Timeframe for delivery (differentiated between outcomes)

# Draft Mandate

- Establish a clear set of required (data) inputs and outputs.
- Examine current and prospective SOC projects & tools.
- Create a reference design for larger sites/sites with experience with a security appliance for smaller sites/those that wish it.

# Participation

---

- Sites
- People

# Participation

- *Sites*
- *Sizes*
  - (T0), T1, T2 (large, medium, small/caching)
- *Types*
  - "Dedicated", Shared

# Participation

- Sites
- Sizes
  - (T0), T1, T2 (large, medium, small/caching)
- Types
  - "Dedicated", Shared
- *People*
  - Expertise + interest!



# Potential technical seed

- **Intrusion Detection Systems + Threat Intelligence**
  - Would provide base from which sites could build
  - Allows us to investigate sharing frameworks in parallel with real data gathering
- **IDS: Bro** [[www.bro.org](http://www.bro.org)]
- **Threat Intelligence: MISP** [[www.misp-project.org](http://www.misp-project.org)]

# Timescales

- Initial timescale
- WLCG Workshop in October
- Central MISP instance + test sites
- IDS guidelines
- Bandwidth/space guidelines for different site types

# Data protection/privacy

- Key note is data protection and privacy
- Proposal: sharing only for threat intelligence with actual log data being exchanged only upon request if and when needed as part of a WLCG security incident investigation
- Liaise with security policy group
- Vital to have input from sites with different topologies and those that share space with non-WLCG users

# Next steps

---

- Call for participation open
- Pre GDB F2F in July + online meeting beforehand

# Contact details

- [wlcg-soc-wg@cern.ch](mailto:wlcg-soc-wg@cern.ch) (open subscription with approval)
- <https://wlcg-soc-wg.web.cern.ch>
- CERNbox area (shared between e-group members)