WLCG SOC WG
Workshop Summary

David Crooks
Liviu Vâlsan

david.crooks@cern.ch
liviu.valsan@cern.ch

WLCG SOC WG Workshop

- In December we held the first WLCG Security Operations Center WG Workshop/Hackathon
- 1.5 days
  - Half day introduction
  - Full day workshop proper

Background

- Build a Security Operations Center reference design, starting with initial model
    - What is happening in my cluster?
        - Network monitoring: IDS
    - What events are taking place that I need to know about?
        - Threat Intelligence

Introduction

- 27 registered attendees (inc. Liviu and David)
  - 17 in person
  - 10 remote
  - 19 institutes
  - 8 countries
  - Most for both days
- Very happy to see everyone

Goals

- Deploy two components of SOC model
  - Threat Intelligence: MISP
  - IDS: Bro
- Integrate MISP and Bro
- Discuss next steps post workshop
  - Activities
  - Future workshops

Goals

- Additionally
  - Good opportunity to look at documentation and other materials
  - Engage with new participants
  - Expand working group

MISP

- Threat intelligence sharing
- Specific areas of work:
  - Deploy MISP
  - Sync events from WLCG MISP instance
    - misp.cern.ch
  - Discuss how MISP might be structured to share threat intelligence in our community

MISP

- Deploy MISP (mostly Tuesday morning)
  - All sites able to deploy MISP after work with provisioning systems
- CERN Puppet modules
  - Masterless
  - Server / client
- http://wlcg-soc-wg-doc.web.cern.ch/wlcg-soc-wg-doc/misp/

MISP

- Sync events from WLCG MISP instance (Tuesday afternoon)
  - Most new instances configured syncing with WLCG instance
  - Some ongoing work to resolve remaining specific configuration
- Questions
  - Access to WLCG instance is via CERN account or eduGAIN+SIRTFI enabled institutional Identity Provider
  - If you're interested for next time and your institution is in eduGAIN but not SIRTFI enabled, talk to your Identity Provider!
  - https://refeds.org/sirtfi

MISP

- Discuss how MISP might be structured to share threat intelligence in our community (also next steps)
    - Institution / NGI / WLCG levels
    - Institution
        - IN2P3 (France)
    - NGI
        - UK

Bro

- Intrusion detection system
- Specific areas of work
  - Discuss network taps / locations
  - Deploy Bro

Bro

- Discuss network taps / locations
  - Discussed CERN configuration and different possible approaches
- Deploy Bro (Tuesday afternoon)
  - Several sites have Bro deployed
    - At least seeing workers running / logs generated
- http://wlcg-soc-wg-doc.web.cern.ch/wlcg-soc-wg-doc/bro/

Bro

- Next steps
  - Continue deployment of Bro
  - Tuning
  - Plan to increase monitored network traffic as experience gained

MISP / Bro Integration

- Script to generate Bro import data from MISP IoCs
  - Tested pulling data from MISP to Bro instances
- Next steps
  - Complete import into Bro
    - Check the alerts!

Next steps

- Successful workshop
- Excellent discussion
- Discussed future workshops: two strands
  - Initial steps for newer users
  - Broader topics for those with more experience

Next steps

- Initial proposal
  - Next workshop in ~6 months
  - Extended to ~2 or so days
- Different blocks include…
  - Initial steps
  - Integration with ELK stacks / ELK security
  - Network configuration
  - Advanced aggregation, correlation and enrichment of generated alerts

Conclusion

- Many thanks to all attendees, in person and remote
- Stimulating discussion
- Very useful work
- Lots more to do!

Conclusion/GridPP

- Straightforward to deploy test MISP
- Encourage sites that are interested to get in touch and use instructions to try a deployment
- Understand the kind of information in events
- How could we use this in the UK?

Contact

- Website
  - wlcg-soc-wg.web.cern.ch
- Mailing list
  - wlcg-soc-wg@cern.ch
- Documentation
  - wlcg-soc-wg-doc.web.cern.ch
- david.crooks@cern.ch
- liviu.valsan@cern.ch