



Incident Response and Threat Intelligence WISE May 2021

David Crooks

Romain Wartel



Overview

- Background
- Status
- IR-TI WG




Incident Response and Threat Intelligence



Background

- R&E organizations are increasingly facing sophisticated groups and APTs
 - They typically do not have the effort, time, resources or skills to deal with this
- R&E organizations share similar user communities and threat actors
 - As a community, we are as weak as our weakest links
 - Highly heterogenous environment
 - Some have a mature SOC and opsec
 - Others may have no experience or procedures in place
- We are targeted as a community:
 - Phalanx/Windingo: 1500+ R&E organisations involved in the same intrusion
 - HPC attacks in 2020: Most HPC centers in EU root compromised, victims in US/Asia
 - Increasing number of community-wide intrusions: Venom, Busywinman, Liquid bigos, Maple Syrup, Smoked Ham, etc.
- Why not defend together?

Incident Response and Threat Intelligence

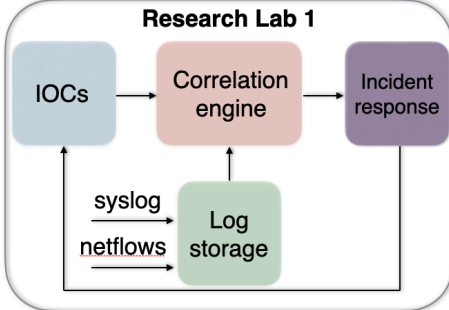


Strategy

1. Leveraging community-based threat intelligence
 - Crowd-source threat intelligence in R&E: targeted, quality, relevant
 - Commercial feeds are useful but: expensive, not necessarily relevant
 - Operate one or more central infrastructure(s) to allow R&E to trust & share

2. Enable R&E orgs to make use of this threat intelligence:
 - Design and integrate a SOC in their local infrastructure
 - Daily security operations relying on a SOC
 - Collect local system and network logs (Zeek, etc.)
 - Correlate it with threat intelligence
 - Take action, incident response
 - Share back (false positive, sightings, additional indicators, samples)

Research Lab 1



```
graph TD; IOC[IOCs] --> CE[Correlation engine]; CE --> IR[Incident response]; LS[Log storage] -- syslog --> CE; LS -- netflows --> CE; subgraph SOC [Security Operations Centre]; IOC; CE; IR; LS; end
```

Threat Intelligence



- SOC WG

- Widened scope since its inception

- Originally WLCG, but now grown to welcome wider R&E participation including from the US and AsiaPacific
 - With WLCG being one specific use case

- Different work strands

- Following a coordination meeting earlier this year, identified some common strands
 - New deployments
 - Experienced deployments developing use of threat intelligence
 - Dockerised deployments for small installs/training/demonstrations
 - High bandwidth networks ($\geq 100\text{G}$)
 - Work to gather **active** participants in these areas



Other SOC efforts

- [OmniSOC](#)
- [ResearchSOC](#)
- [Science DMZ](#)

- Heard about work at UNINETT this morning

- Different models, but keen to coordinate and share experience

Incident Response



- Work ongoing around operational security in global R&E
 - Share soon – stay tuned!
- Essential that operational security teams are involved with threat intelligence work

WISE IR-TI



- We have work ongoing in different groups to carry out this work at an operational level
 - Shouldn't repeat that at WISE, BUT
- Could use this forum both to give status updates of the various work and coordinate between groups
 - If someone is looking to start a new endeavour, is there something that could be expanded to include that to avoid splitting effort?

SOC WG



- David Crooks (david.crooks@stfc.ac.uk)
- Liviu Vâlsan (liviuvalsan@cern.ch)

- Website: wlcg-soc-wg.web.cern.ch
- Documentation: wlcg-soc-wg-docs.web.cern.ch
- Mailing list: `wlcg-soc-wg [at] cern [dot] ch`



Thank you - questions?