Harnessing the power of threat intelligence for WLCG cybersecurity

WLCG Security Operations Center Working Group

David Crooks, Liviu Vâlsan

CHEP 2019, Adelaide, November 2019
Overview

- Background
- Technology stack
- Threat intelligence
- Recent progress
- Next steps
- Summary
- Contact details
As discussed at CHEP 2018, the WLCG SOC WG is mandated to create reference designs to allow WLCG sites to

- Ingest security monitoring data
- Enrich data, store and visualize
- Alert based on matches between this security data and threat intelligence (Indicators of Compromise or IoCs)
In this talk we discuss the following areas of work:

- Technology stack
- Best practices for use and sharing of threat intelligence
Technology stack: Initial Model

**Data sources & threat intelligence**
- **MISP**
  - Threat Intelligence Sharing
  - Essential

**Data pipelines**
- **Zeek (Bro)**
  - Intrusion Detection System
  - Deep Packet Inspection
  - Optional
- **Logstash pipeline**
  - JSON logs
  - Filebeat

**Storage & visualisation**
- **Elasticsearch**
  - Real Time Indexing
  - Essential
- **Kibana**
  - Visualisation
  - Essential

**Alerting**
- **Enrichment, correlation, aggregation**
  - Optional
- **Elastalert**
  - Optional

**Data sources & threat intelligence**
- **netflow/sflow**
  - Network flow metadata
  - Optional

Choose at least one data source

Choose at least one alert method
Storage & visualisation

MISP
Threat Intelligence Sharing
Essential

Elasticsearch
Real Time Indexing
Essential

Elastalert
Optional

Kibana
Visualisation
Essential

Data sources & threat intelligence

Zeek (Bro)
Intrusion Detection System
Deep Packet Inspection
Optional

netflow/sflow
Network flow metadata
Optional

Elasticflow
Enrichment, correlation, aggregation
Optional

Alerting

Choose at least one data source
Choose at least one alert method
## Technology stack: initial model

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

• This summer, two new SOC prototypes under development:
  – Nikhef: Zeek data source (OpenPOWER8)
  – STFC Cloud: sFlow from subset of hypervisors

• At the recent SOC Workshop in Nikhef (21-21 October), demonstrated SOC workflow:
  – Trigger activity at CERN (using EGI CSIRT SSC framework)
    • Create MISP event
  – Check the propagation of this threat intelligence to STFC
  – Trigger same activity at STFC
    • Check this is seen/alerted on

• Successful demonstration and important milestone
• 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

CHEP 2019, Adelaide
# Code of conduct: TLP

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED</td>
<td>Not for disclosure, restricted to participants only</td>
</tr>
<tr>
<td>AMBER</td>
<td>Limited disclosure, restricted to participants’ organizations</td>
</tr>
<tr>
<td>GREEN</td>
<td>Limited disclosure, restricted to the community</td>
</tr>
<tr>
<td>WHITE</td>
<td>Disclosure is not limited</td>
</tr>
</tbody>
</table>
• Lead to 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
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

• Document on guidelines for access to CERN instance to be prepared this year
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
  – wlcg-soc-wg-doc.web.cern.ch

• Egroup
  – wlcg-soc-wg@cern.ch

• David Crooks (david.crooks@cern.ch)

• Liviu Vålsan (liviu.valsan@cern.ch)

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