Security Operations Centres WG

Status Report

David Crooks and Liviu Vâlsan

wlcg-soc-wg@cern.ch

GDB, 14th December 2016

Overview

- Update on progress in Security Operations Centres working group
  - (particularly following meeting on 8/12)
- Strategy
- Next steps

Roadmap

- Since earlier this year, developed strategy of building systems from smaller building blocks
  - SOCs are complex with components in several domains (data gathering, processing, storage…)
- Minimum viable product
  - Threat intelligence: MISP
  - IDS: Bro
  - Reference framework: Metron

Bro

- Open Source Network IDS (intrusion detection system) in broad use

- Strong use in the US

- Area where Europe could maybe benefit from more investigation

Bro [status]

- Bro under investigation by several sites in the working group
  - Durham working through deployment issues; data capture & volume
  - 10-15 GB/day (raw) on 4 Gb/s connection
  - Currently offline for investigation of network switch performance issues
  - Brunel is working with Bro as well; future report
- Planned to extend deployment to other sites, including Glasgow, in the New Year
  - Hardware earmarked
- Option to monitor worker nodes through NAT as first step

MISP

- Threat intelligence sharing

- See previous GDB talks

MISP [status]

- Test deployment at RAL and Glasgow, including synching of test data

- Tested synchronisation between WLCG to Glasgow MISP instances

- Tested giving access to Glasgow Campus Security

MISP + SIRTFI

- Glasgow added to UK Access Federation SIRTFI pilot
- Enable direct access to institution security team to WLCG instance
  - Useful to explore different access methods and routes
- Ian Neilson talking to RAL Campus Security Team in New Year

MISP training

- Two MISP training events since last report
  - Brussels and Zurich; latter including hackathon
- Good materials - good to have developer input
- Overview of product landscape + capabilities

CERN update

- Alls IoCs from MISP being fed into Bro
  - False positives were an issue to be solved; careful work to resolve
    - Small number of attributes potentially accounting for large number of false positives. (eg URL shorteners)
  - Initially tens/hundreds notifications/day (on 30-40k devices)
  - Now, 5-20 notifications/day total in general
  - Last 30 days of MISP IoCs exported to Bro (sliding window)
  - Examples of false positives:
    - IPs hosting many domains (CDNs, web hosting providers, etc)
    - Scans from IPs hosting Command and Control servers scanning the network generating alerts (work ongoing to raise notifications based on direction of traffic)

Next steps

- With more experience with MISP + Bro:
- Add more sites with Bro; different network layouts and storage needs…
- Work towards integrating MISP with Bro at non-CERN sites
- More SOC components - Elasticsearch, etc.