IR-TI
SIG-ISM/WISE
April 2022
David Crooks
Romain Wartel
Overview

• Approach
• SOC WG progress
• pDNS and IR exercise update
• Contact
Approach

- Source of threat intelligence
  - **Central R&E MISP instance** (hosted at CERN)

- Technical collaboration
  - **SOC WG**

- High level coordination
  - **WISE IR-TI**

- Global operational security
  - **EGI CSIRT, OSG Security, SAFER**

- Collaboration and cooperation with other initiatives
  - **GEANT, ...**
SOC WG recent progress

• EGI CSIRT building MISP into IR procedures
  • Important step in integration into our current procedures
    • Driver for adoption of threat intelligence sharing
  • See later this session

• Early stages of Kubernetes-based SOC
  • Training, demonstration and small site deployments
  • Broader context of cloud-based sites
  • Laying foundations for long term development
Kubernetes SOC

• Design principle: every component can be chosen independently
  • Zeek, OpenSearch, MISP...
• Aim at production quality configuration
• Full control over configuration of system according to needs
  • providing sane defaults for testing and training
• Goal: same base OS for all images, similar design → ease of use
• Creating images which adhere to the design principles.
  • Currently working on MISP
• Kubernetes deployments
  • Following the design principles
  • Applying best practices and modern build processes
Nikhef SOC

• Focus on SOC 'services': ELK/Visualisation/etc moved to HA configuration
  • Working to increase number of threat feeds
  • Like to move from Zeek Intel alerting to Elastalert
    • Needs custom Zeek export
STFC SOC

• Hardware and networking in place with optical taps available for 2x100G Janet links + 100G LHCOPN
  • Working on deployment step based on security-focused config management baseline
  • 3 graduates working on this and related projects this summer
  • Sharing deployment information with Jisc
    • Presented at recent 100G networking meeting
    • Session at Networkshop50
pDNS SOC

• Lowering the barrier for sites to gain SOC capabilities without deploying a dedicated facility
• Focus on passive DNS data
  • Detect traffic to well-known malicious websites
  • Used in incident response lifecycle
  • Historical details beyond standard DNS
• Current state
  • pDNS Sensor data ingestion design
  • pDNS data - MISP threat intelligence correlation engine design
  • Interface for searching queries
Incident response training exercise

• Preparations underway
• More to follow
Contacts

• David Crooks (david.crooks [at] stfc.ac.uk)
• Liviu Vâlsan (liviu.valsan [at] cern.ch)
• Romain Wartel (romain.wartel [at] cern.ch)
• Christos Arvanitis (christos.arvanitis [at] cern.ch)
• Pinja Koskinen (pinja.koskinen [at] cern.ch)

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