SOC WG: GDB

12th of April 2023

David Crooks

Liviu Vâlsan

Agenda

- Intro to the working group
- Status update
- Training
- Next steps

Security Operations Centres Working Group

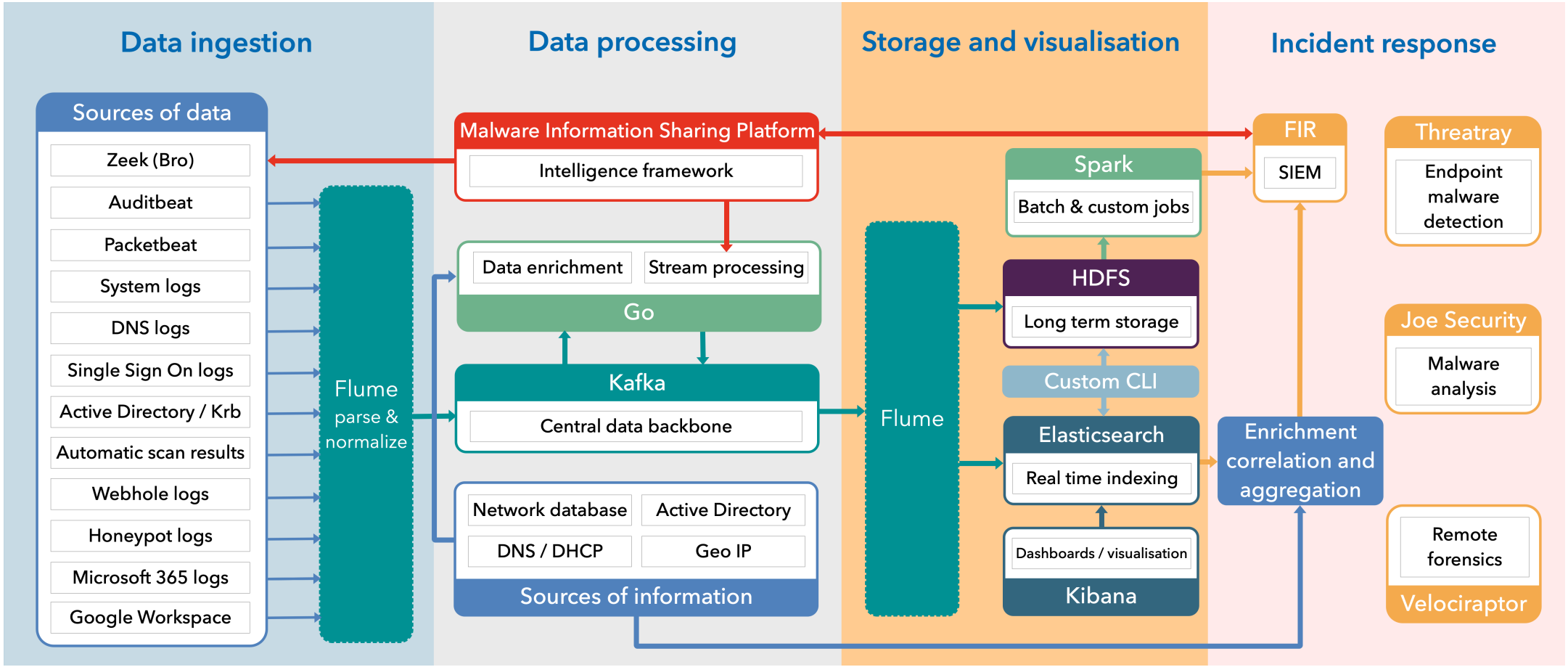
- Allowing WLCG sites to digest and make active use of threat intelligence is a cornerstone of the WLCG security strategy
- The WLCG Security Operations Centre WG was established to enable the deployment of security tools to enable this
  - But also including members from the wider academic research community

- The working group is mandated to create reference designs to allow sites to
  - Ingest security monitoring data
  - Enrich, store and visualize this security data
  - Alert based on matches between the stored data and threat intelligence
  - Indicators of Compromise or IoCs

STFC Deployment

- New Scientific Computing Security Operations and Engineering Team now in place with 3 engineers (+David Crooks) to support this work
- Hardware/networking in place
- New configuration management template completed to support security-first config
- Config managed deployments of Zeek, OpenSearch and MISP in testing
  - Kafka to follow Opensearch
- Data now flowing from LHCOPN tap to zeek node

CERN Deployment



CERN Deployment

- Migrated from Elasticsearch to Opensearch
  - Lots of optimisations with respect to Opensearch
- New data sources added
  - Working at integrated cloud logs (Microsoft Azure and Google Workspace / GCP)
- Revamp of Incident Response toolkit

Nikhef Deployment

- After the migration of our core routing which is happening soon™, **all** links will be monitored
- The network sensor will get a RAM upgrade to allow tracking of these extra connections
- Custom elastalert/MISP combo is working
- Some hardware shuffling will also happen with the hopes of improving Elasticsearch performance, stability and reliability

USATLAS Deployment

- Two WLCG SOC related milestones:
  - WLCG SOC instance operational at AGLT2 in April 2023.
  - MWT2 operational instance in May 2023.
  - Planning to attend the upcoming WLCG SOC Hackathon in person.
- Both AGLT2 and MWT2 have purchased NVIDIA Bluefield-2 100G dual-ported NICs
  - Investigating how to utilise these these cards to help Zeek with the data capture process
- Looking to have the capture hosts, Zeek and MISP hosts EL9 based.

Training

- In June 2022, first security focused thematic CERN School of Computing took place.
- This included a 3h workshop using a bare bones SOC deployment
  - New version of PocketSOC (for those that recall)
  - Multiple containers with traffic monitored by zeek container
- Deployed on CERN openstack
  - 36 instances
  - Allowed SOC functionality to be explored
  - New version now in development to allow for easier cloud deployment

Next Steps

- Continue working with larger sites to deploy SOC capabilities
  - Refresh call for Tier1s that are interested in this
- Planning a significant piece of work in the UK around the UK Research and Innovation Digital Research Infrastructure programme
  - DavidC leading the DRI Cybersecurity project and UKRI SOC working group and will be encouraging research organisations across the UK – including UKRI councils – to participate in the working group
- Refresh documentation and guidance with RHEL8/9 in mind
- New technologies and techniques: Bluefield, distributed secure messaging...

Next Steps

- SOC Hackathon
  - Taking place at Cosener's House, Abingdon, UK
  - Week commencing 14th of August 2023
  - Registration is open!
  - https://indico.cern.ch/event/1268239/

- Broad work on global TI sharing and sharing of common approaches
  - Part of GEANT 5-1 project

WLCG SOC WG

- David Crooks (david.crooks@stfc.ac.uk)
- Liviu Vâlsan (liviu [dot] valsan [at] cern [dot] 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