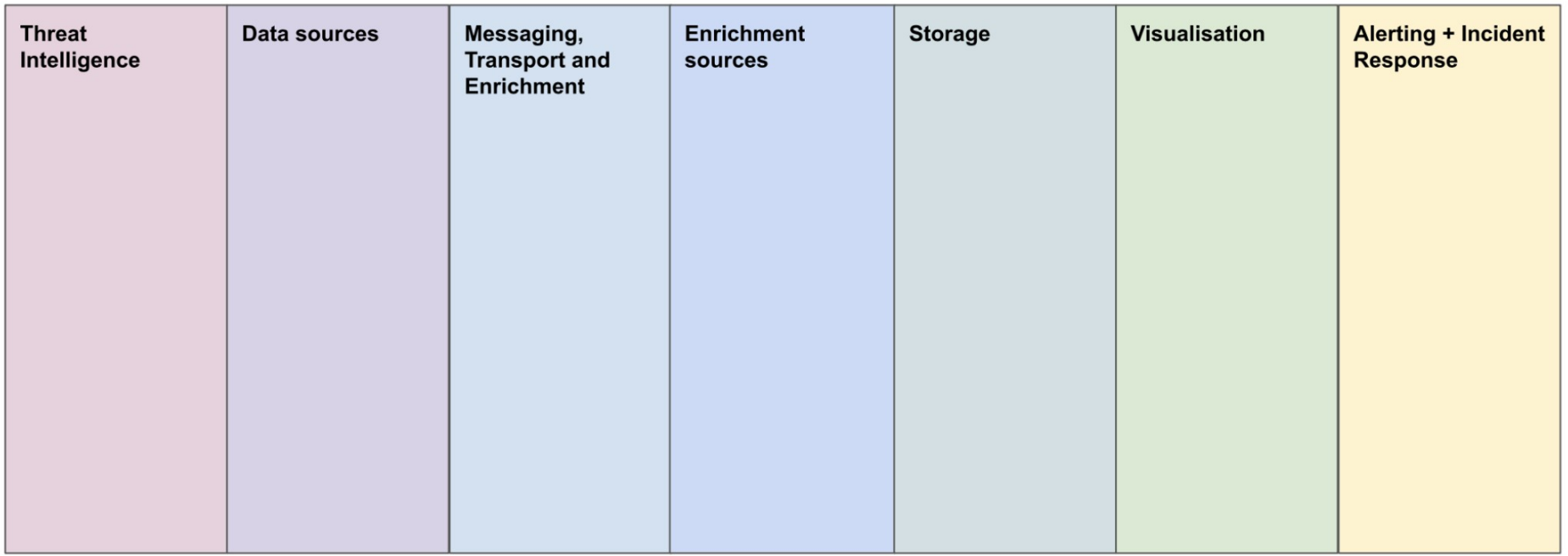
Deploying Security Operations Centre capabilities

David Crooks, Liviu Vâlsan, Liam Atherton

Overview

- SOC Models
  - SOC WG Reference model
  - Full-scale: deep packet inspection
  - Lightweight: Correlation of DNS logs with threat intelligence
- Current use cases (full-scale): CERN + STFC
  - CERN example
  - STFC example
- Future use case: GridPP/Lancaster
  - Unicor

Reference Design



SOC Models [1]

- Lightweight
  - Focus on specific existing log sources
  - Correlation of DNS logs with threat intelligence
  - Allow for deployment of correlation engine locally or remotely
  - Does require access to threat intelligence, but access to remote MISP with API key sufficient
  - Can be deployed with external security team supporting local responders if appropriate

Unicor

- Based on pDNSSOC
- Correlating logs with threat intel from MISP
  - Unicor provides a turn-key solution to detect and respond to security incidents
- The basics:
  - Source DNS logs or JSON input, and Unicor correlates this with suspicious/malicious domains, synced from one or more MISP instances
  - Alert sent to configurable destination based on a template
  - Includes grouping of alerts, rate limiting, deduplication, and… retro-searches!
- Started as a poor man’s SOC. Becoming a generic contextualization and alerting platform.
- https://github.com/safer-trust/Unicor

Future use-case: Unicor

- GridPP project in the UK
  - UK component of worldwide LHC computing activity
- Plan to deploy Unicor at set of larger Tier-2 sites
  - Tier-1 located in RAL: STFC
- Initial pilot: Lancaster
  - Initial deployment plan discussed beginning of 2026
  - Preliminary implementation steps in place
  - Planning deployment around other priorities
  - Focus on grid site DNS forwarder in first instance

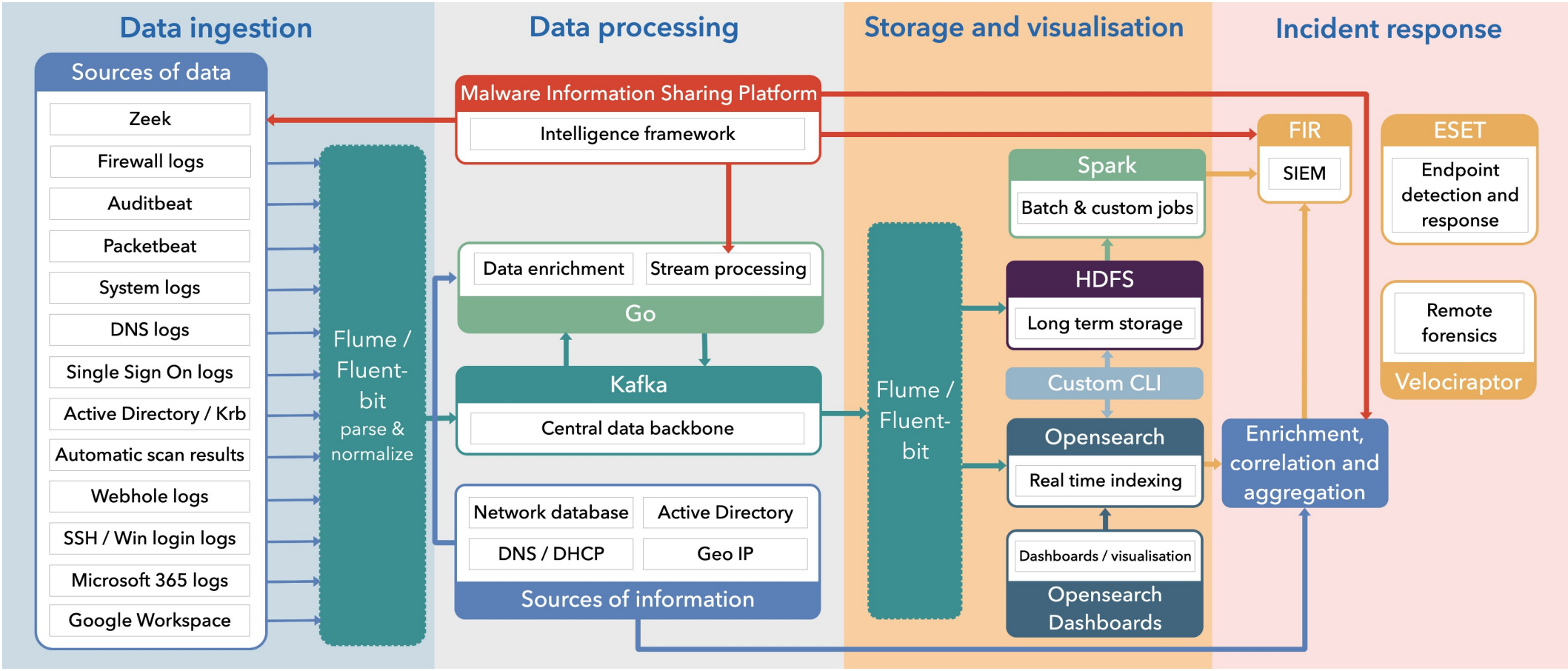
Unicor pilot goals

- Focus on detection capabilities that the project can offer to hosting organisations/community
- Part of overall set of activities
- Support parallel activity on site security posture
- Feedback on useful deployment mechanisms in our environment
  - Including packaging

SOC Models [2]

- For sites operating at 100+ Gb/s: deep packet inspection
  - Passive mirroring of designated traffic streams
  - Optical taps/port mirroring/…
  - Ingestion of analysis logs, correlated with threat intelligence, to storage and visualisation
  - Alerting

CERN Outline

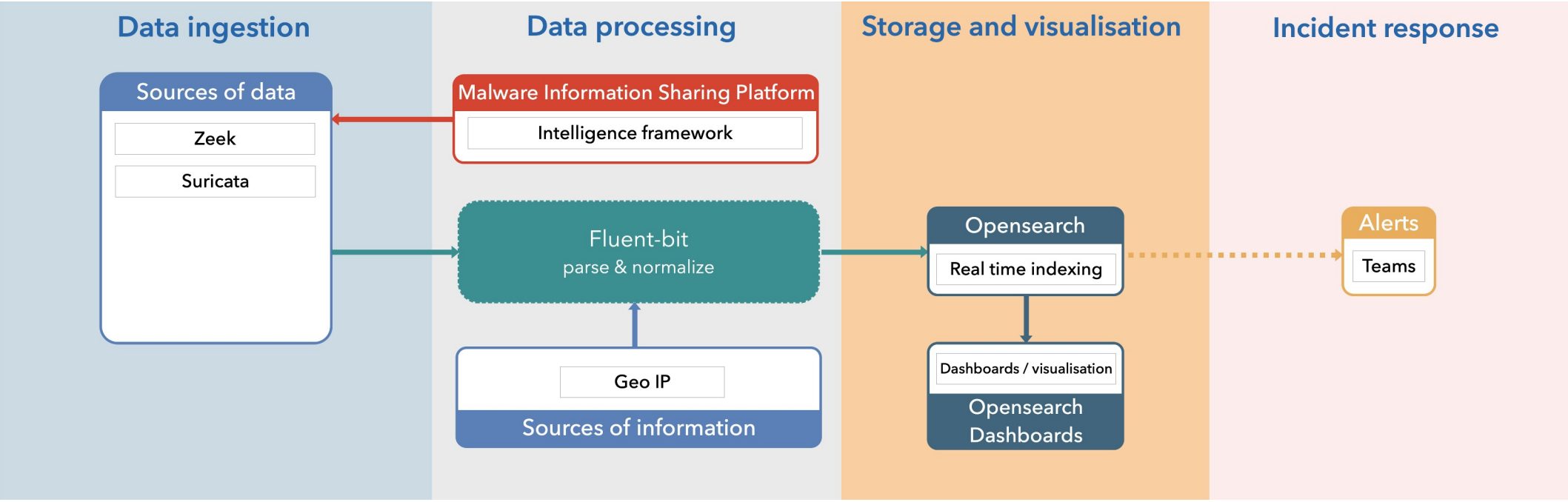


CERN status

- Monitoring the following:
  - Internet traffic from the CERN internal network to the Internet (400 Gbps)
  - Traffic between the General Purpose Network and the Technical Network
  - Guest WiFi network
  - Traffic going to all DNS servers, both internal and external servers
  - Detailed traceability (command execution / network) for batch (grid) clusters and interactive clusters
  - Different sources acting as complementary / redundant (e.g. Zeek and firewall logs)

STFC Outline

Science and Technology Facilities Council
Scientific Computing



STFC updates

- **All** Janet and LHCOPN links now being monitored
  - 10 individual 100 Gb/s links
  - 4 x 100 Gb/s Janet primary/secondary
  - 2 x 100 Gb/s LHCOPN
- **Suricata** now deployed across the capture cluster in parallel with Zeek
  - Adding signature based detection capability to existing fine-grained networking monitoring
  - Ongoing characterisation
- Capture loss has improved to < 1% to a few %

Lessons learned

- Minimum viable product
  - When building up capabilities, have MVP in mind
  - Well characterised, smaller set of data sources to start
  - Ensure existing sources are well-exploited before adding new ones
    - Having logs doesn’t mean you should use them
- “We have lots of logs can you ingest them?”
  - What value would this information add to cap[ability?
- Only deal with logs/telemetry with security benefit

Lessons learned

- Development needs to take in place with target audience in mind
  - And takes place in the existing environment
- Try to build on top of existing technologies/services where they exits
  - For example CERN OpenSearch service
  - Follow existing business practices
  - Alerts and ticketing should follow existing tools where they exist
    - Ultimate decisions should reflect this

Threat Intelligence Workshops

- Set of online workshops co-hosted by SOC WG and SAFER-TRUST
- Aim to have working MISP setups by end of workshops
  - “Office hourse” put in place in advance to answer tech questions
  - Workshops focus on detailed configs
- Most recent was 25th February 2026
  - https://indico.cern.ch/event/1596660/

Getting involved

- SOC WG has an online community
  - Mailing list
  - Keybase team
- Please get in touch if you're interested in joining
- Primary website
  - wlcg-soc-wg-doc.web.cern.ch
- Regular hackathons
  - Next likely to be in UK beginning of September
  - Looking for distinct workstreams for this meeting

Conclusion

- Pilot now underway to use Unicor to correlate DNS logs with threat intelligence
  - Intent to deploy more broadly in the UK and inform WLCG options
- STFC now monitoring all RAL links and added Suricata to data sources
- Lessons learned informed by “real world” deployments in existing environments, informed by security needs