WLCG
Worldwide LHC Computing Grid

WLCG Security Operations Centres Working Group

David Crooks and Liviu Vâlsan
for the WLCG SOC WG

wlcg-soc-wg@cern.ch
wlcg-soc-wg.web.cern.ch

ISGC, March 2017

Overview

- Context
- Security Operations Centers
  - CERN SOC
- Technologies
- Status
- Conclusions & Future work

Context

- Increasingly complex security environment
- Increasing use of clouds and other virtualised resources
- Work on appropriate security tools needs to keep pace

Security Operations Centers

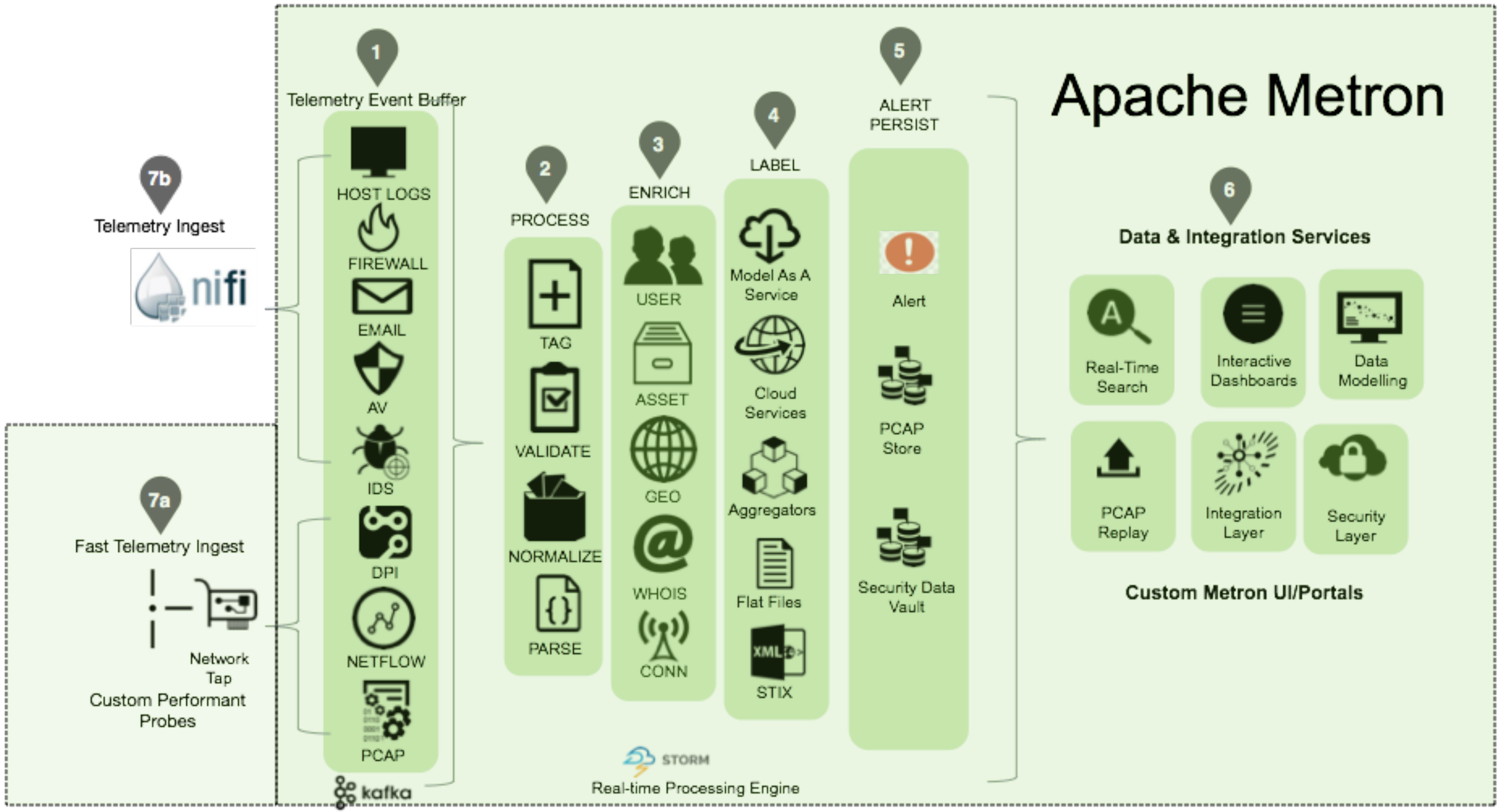
- Analytics is an established field with growing importance
- Apply these concepts to security platforms
- Security Operations Centers (SOCs)

Security Operations Centers

- SOC WG Mandate
  - *Establish a clear set of desired data outputs and necessary inputs.*
  - *Create a scalable reference design applicable for a range of sites by examining current and prospective SOC projects & tools.*

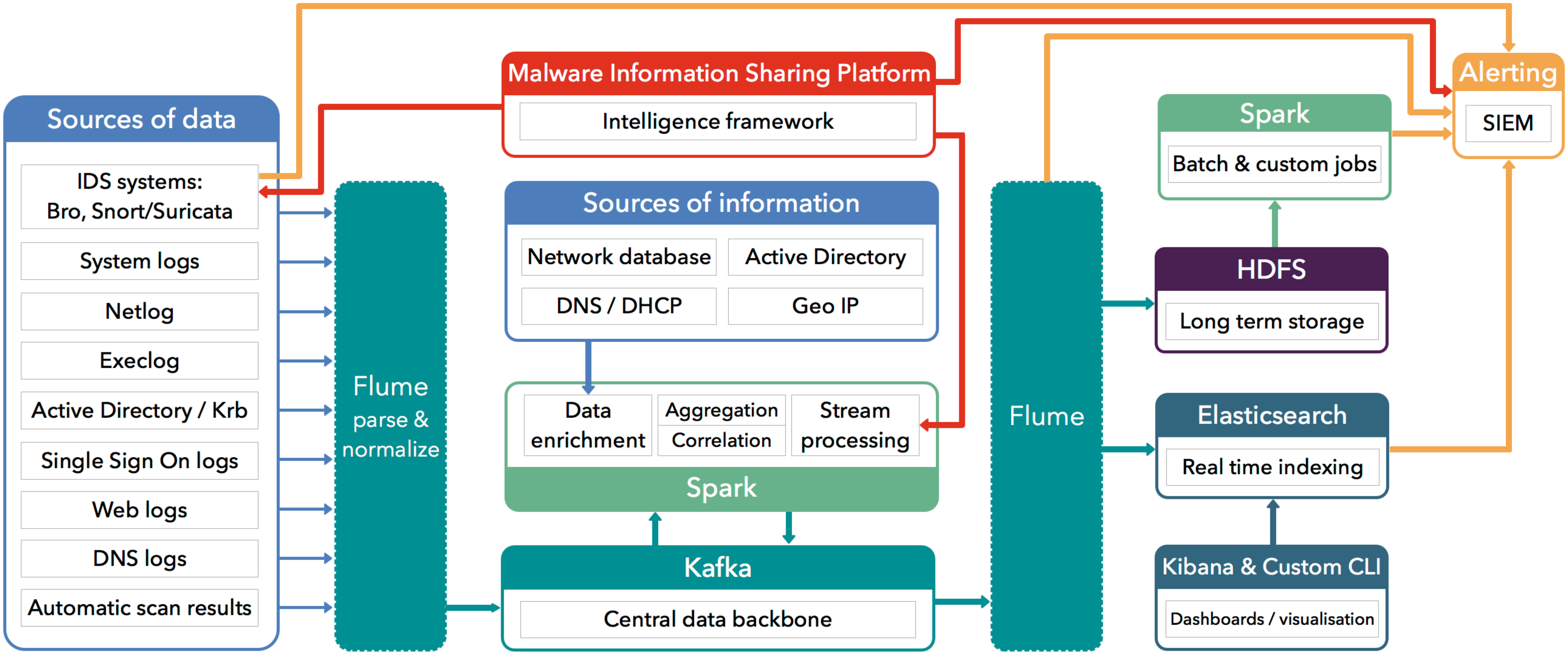
Security Operations Centers

- SOCs can be very complex, employing a large number of tools



http://metron.incubator.apache.org

CERN SOC


Sources of data
IDS systems:
Bro, Snort/Suricata
System logs
Netlog
Execlog
Active Directory / Krb
Single Sign On logs
Web logs
DNS logs
Automatic scan results
Flume
parse &
normalize
Malware Information Sharing Platform
Intelligence framework
Sources of information
Network database
Active Directory
DNS / DHCP
Geo IP
Data
enrichment
Aggregation
Correlation
Stream
processing
Spark
Kafka
Central data backbone
Flume
Spark
Batch & custom jobs
HDFS
Long term storage
Elasticsearch
Real time indexing
Kibana & Custom CLI
Dashboards / visualisation
Alerting
SIEM

CERN SOC

- 100s of GB/day
- Varied range of data
- Built on top of existing CERN IT services whenever possible
- Lessons for other sites (while not necessarily at the same scale)

Technologies

- Given complexity, how best to proceed?
- Minimum viable product
  - What set of tools is effective and allows growth?
- Threat Intelligence
  - MISP
- Intrusion Detection System (IDS)
  - Bro

Threat Intelligence

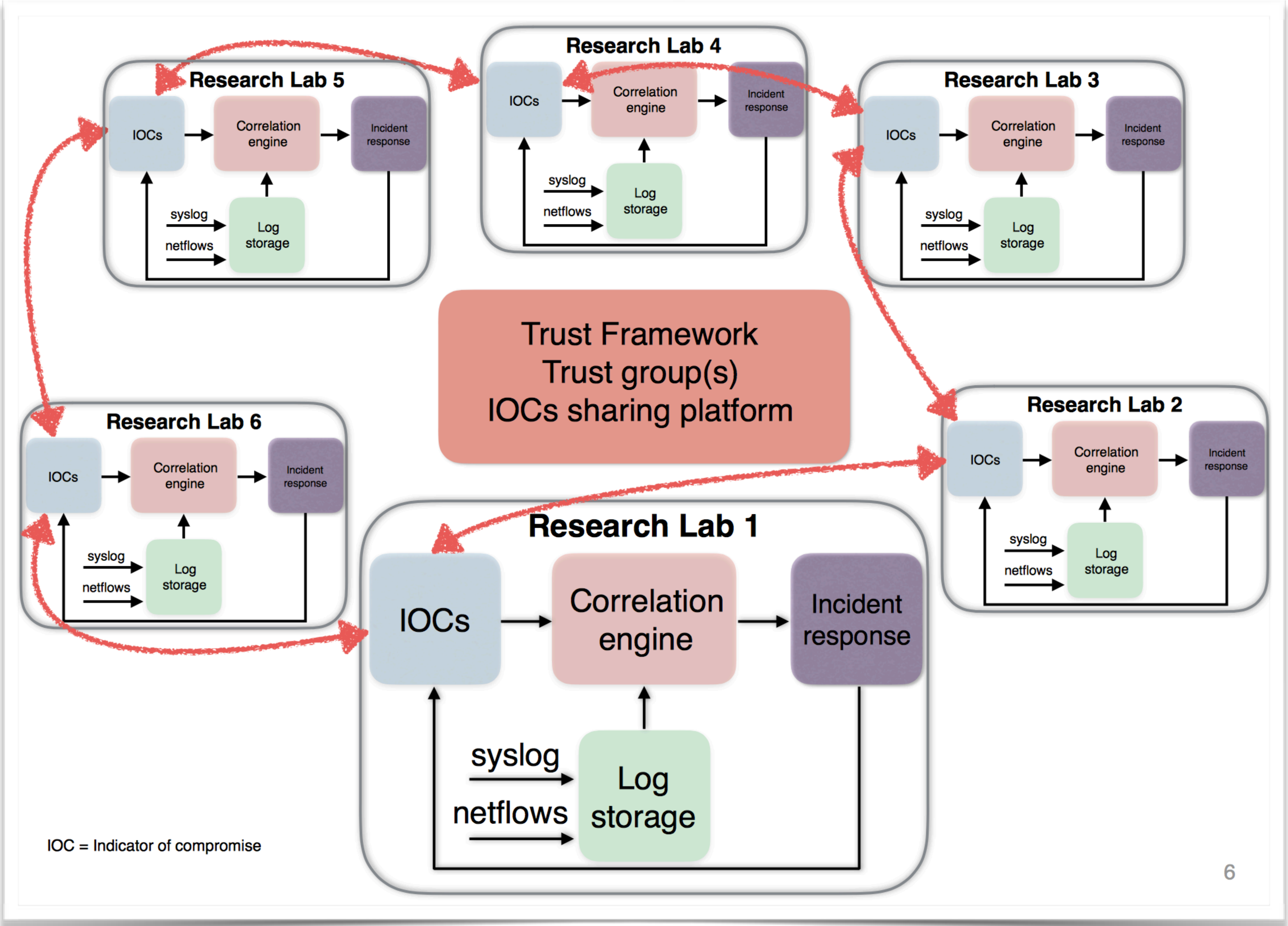
- As a community, threats apply to us all - shared responsibility

- Need to share intelligence to improve ability to respond in a timely fashion

- *The future of academic security*

  - http://indico.cern.ch/event/505613/contributions/2227689/attachments/1349009/2047093/Oral-109.pdf

Threat intelligence



Trust Framework
Trust group(s)
IOCs sharing platform

IOC = Indicator of compromise

- http://indico.cern.ch/event/505613/contributions/2227689/attachments/1349009/2047093/Oral-109.pdf

ISGC, March 2017

MISP

- Malicious Intelligence Sharing Platform

- "A platform for sharing, storing and correlating Indicators of Compromises of targeted attacks. Not only to store, share, collaborate on malware, but also to use the IOCs to detect and prevent attacks."

- Allows development of trust frameworks between sites to allow rapid sharing of threat intelligence

- misp-project.org

Bro

- “Bro is an open-source network security platform that illuminates your network's activity in detail, with the stability and flexibility for production deployment at scale.”
- Strong use in the US
- bro.org
- Act as partner to MISP
  - Ingesting IoCs

Bro

- Scalable
    - Build Bro cluster with worker nodes to expand capabilities
- Important part of work to explore requirements for different sizes and types of sites
    - Network topology

PF_RING

- Part of scalability is running multiple instance of Bro across network interface
  - PF_RING (http://www.ntop.org/products/packet-capture/pf_ring/)
  - Needs to have support compiled into Bro or to make use of the dedicated PF_RING Bro plugin
  - CERN has suitable RPMs available:
    - http://linuxsoft.cern.ch/internal/repos/sec7-external/

Status

- CERN SOC status
- MISP status
- Bro status

CERN SOC status

- Mirrors all traffic before firewall level to Bro
- Working on network device that aggregates traffic from multiple devices
  - with this able to monitor traffic through and bypassing firewalls

CERN SOC

- 450000 IoCs in total in the CERN main MISP instance
  - 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)
  - Tens/hundreds notifications/day (on 30-40k devices) reduced to 5-20 notifications/day total in general

CERN SOC status

- Last 30 days of MISP IoCs exported to Bro (sliding window)
- Still some work ongoing on next steps beyond Bro
  - Layers of the stack: log transport + data backbone (Flume + Kafka), storage, indexing, visualisation (HDFS, ElasticSearch)
  - A large number of bottlenecks already identified and resolved, some tweaks still needed to be able to process the whole amount of data

MISP status

- WLCG MISP, in place at CERN, accessible once added as a user with CERN credentials, and to institutions with SIRTFI enabled Identity Providers.
- Sharing 150k IoCs

MISP status

- Wider WG
  - Installed at Glasgow; work at RAL last year
  - In Glasgow used to share WLCG data with local campus security (early investigation) - sync data with CERN credentials, then give local access to campus personnel
  - Investigations at other sites including Edinburgh

Bro status

- Investigations underway or planned at a number of sites beyond CERN
  - Brunel, Durham, Lancaster, Glasgow

Bro status

- Brunel
    - Investigating working with CISCO Nexus switches/Netflow
- Durham
    - On-switch network mirror
    - Mirroring 4Gb/s WAN link
    - 10-15 GB/day logs
    - currently degrades overall network performance so run periodically

Bro status

- Lancaster
  - Planning to test deployment with CERN RPMs
- Glasgow
  - On-switch network mirror (Extreme x670)
  - Initial test over 3 days; 1 GB compressed logs but showing capture loss: under investigation
  - Testing showed packet loss on outbound WAN link; active investigation of where this comes from

Conclusions

- SOCs are complex

- Following roadmap of small number of components with key benefits

- Expand components over coming months (elasticsearch integration, storage, visualisation)

Conclusions

- MISP installations and sync tested; looking at how to work with data outside CERN
- Bro installations tested; clear dependence on scale and network detail - looking to gain experience
- Promising first stage but more progress needed; more interest welcome