Security Operations Workshop

Security Operations Workshop

- Agenda for today

- 90 minutes now, 180 minutes this afternoon in the “hackathon” session

- Morning [0900-1030]
    - impetus and drivers
    - mini intros to some key tools
    - status update from Chicago + discussion

Security Operations Workshop

- Afternoon [1330-1500 + 1530-1700]

- Technical topics decided on by the group
    - SNMP issues
    - Zeek alerting deep dive
        - Come out with *documented* code snippets!

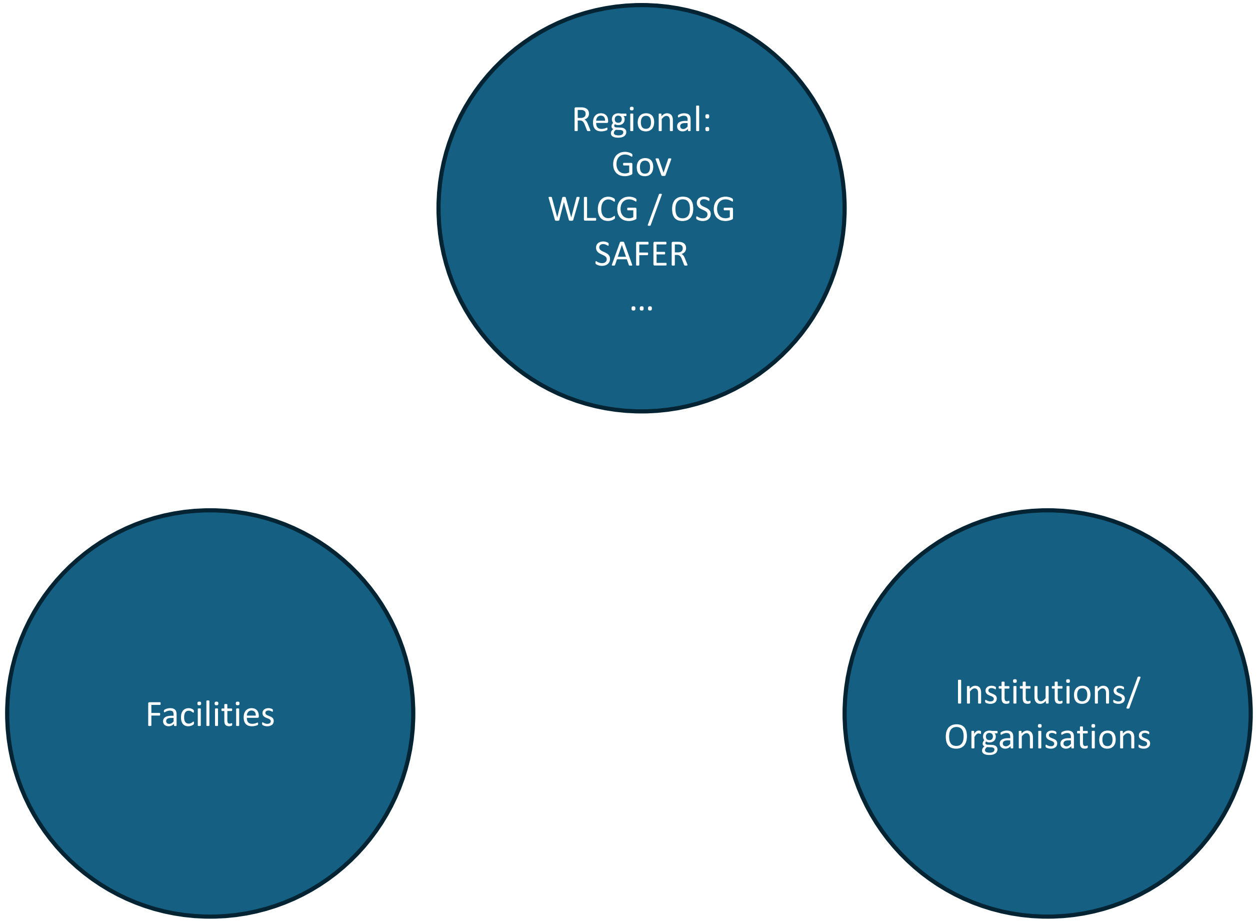
    - Advanced Zeek usage + incident response

- Try to identify other topics before lunch to help prep

What is the scope of our work?

- We must work together to improve the cybersecurity posture of our organisations and infrastructures.
- Before focusing on operational security tools, pause to consider the full scope of the work to be done in this area
- Must have clear picture of this scope, and then make a plan to execute.

Scope


Regional:
Gov
WLCG / OSG
SAFER
…
Facilities
Institutions/
Organisations

Impetus

- Why is this work important?

- Cyber Threat Intelligence (strategic + operational) is fundamental to help us defend as one
  - Strategic -> Landscapes, long term risk analysis
  - Operational -> o(real time) support for incident response + protection

- Both as part of Protection + Response, must use intelligence effectively
  - How to do that might depend on the layer

Roles

- Important when working in this area to consider
  - What is important?
  - Who is best able to take on a role?

Developing strategy and plans

- Introduce two tools that could be of use in building a vision and strategic plan for an organization – or infrastructure

- Trusted CI Framework

- NIST Cybersecurity Framework
  - (as example; other frameworks exist!)

Trusted CI

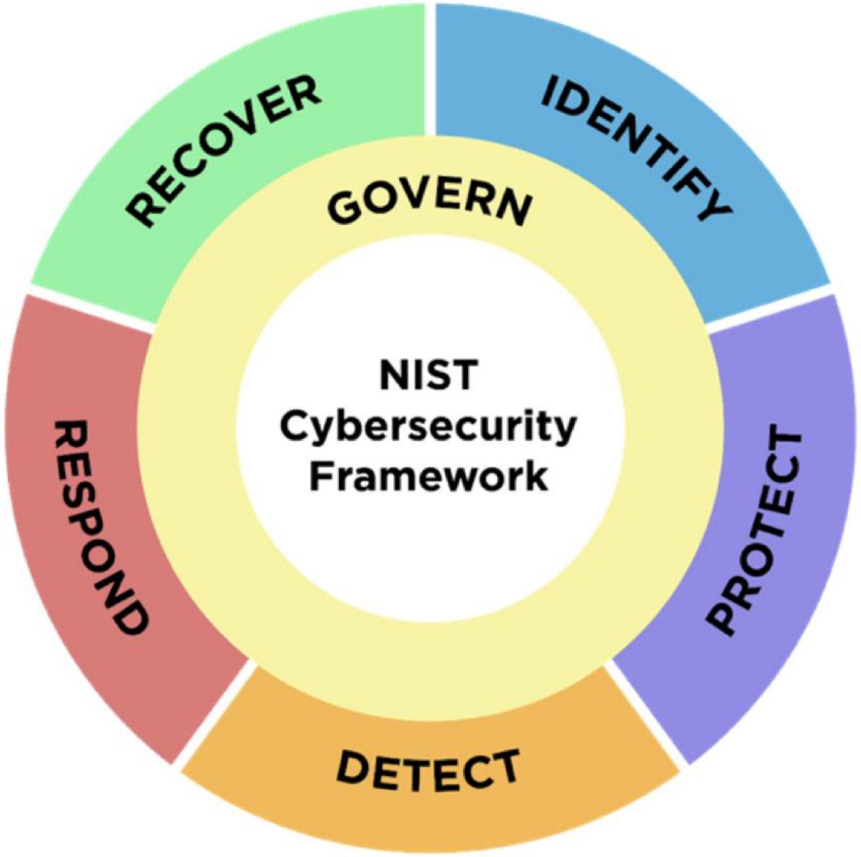
- Trusted CI is the NSF Cybersecurity Center of Excellence
- Cybersecurity experts with experience working with US science and engineering communities
- The team draws from best operational practices and includes leaders in the research and development of new methodologies and high-quality implementations.

Trusted CI Framework

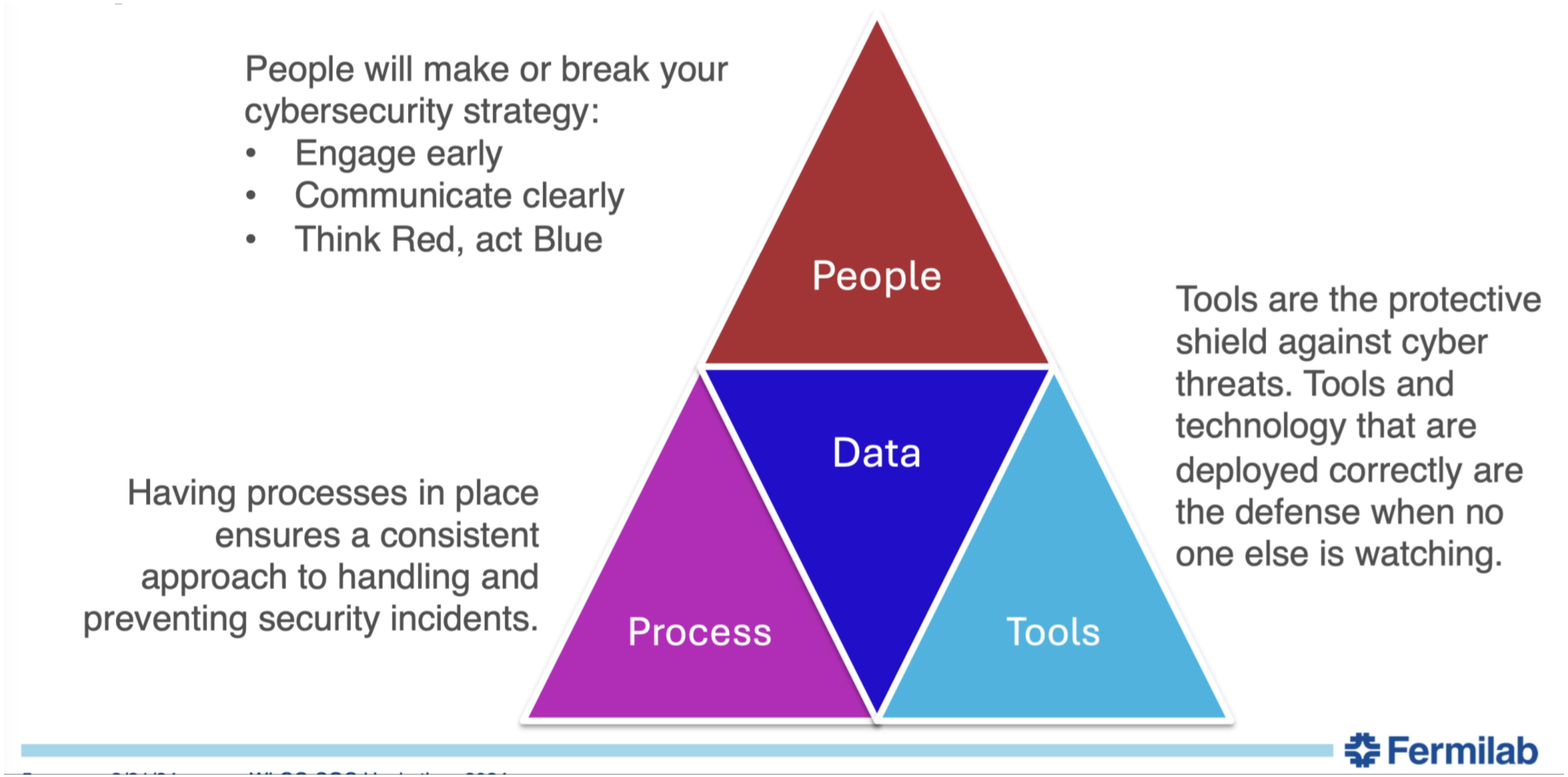
- Trusted CI Framework
  - An approach to support organisations building cybersecurity programmes and strategic plans. Specifically agnostic of other cybersecurity frameworks and technology, this could be of interest for the DRI
  - Representation on Advisory Board by Dave Kelsey on behalf of the WISE Community
    - International involvement
  - 4 pillars: Mission Alignment, Governance, Resources, and Controls
  - 16 “Musts”: Concrete requirements for establishing a cybersecurity program

NIST Cybersecurity Framework

- GOVERN
- IDENTIFY
- PROTECT
- **DETECT**
- RESPOND
- RECOVER



People, Process, Tools and Data



People will make or break your cybersecurity strategy:

- Engage early
- Communicate clearly
- Think Red, act Blue

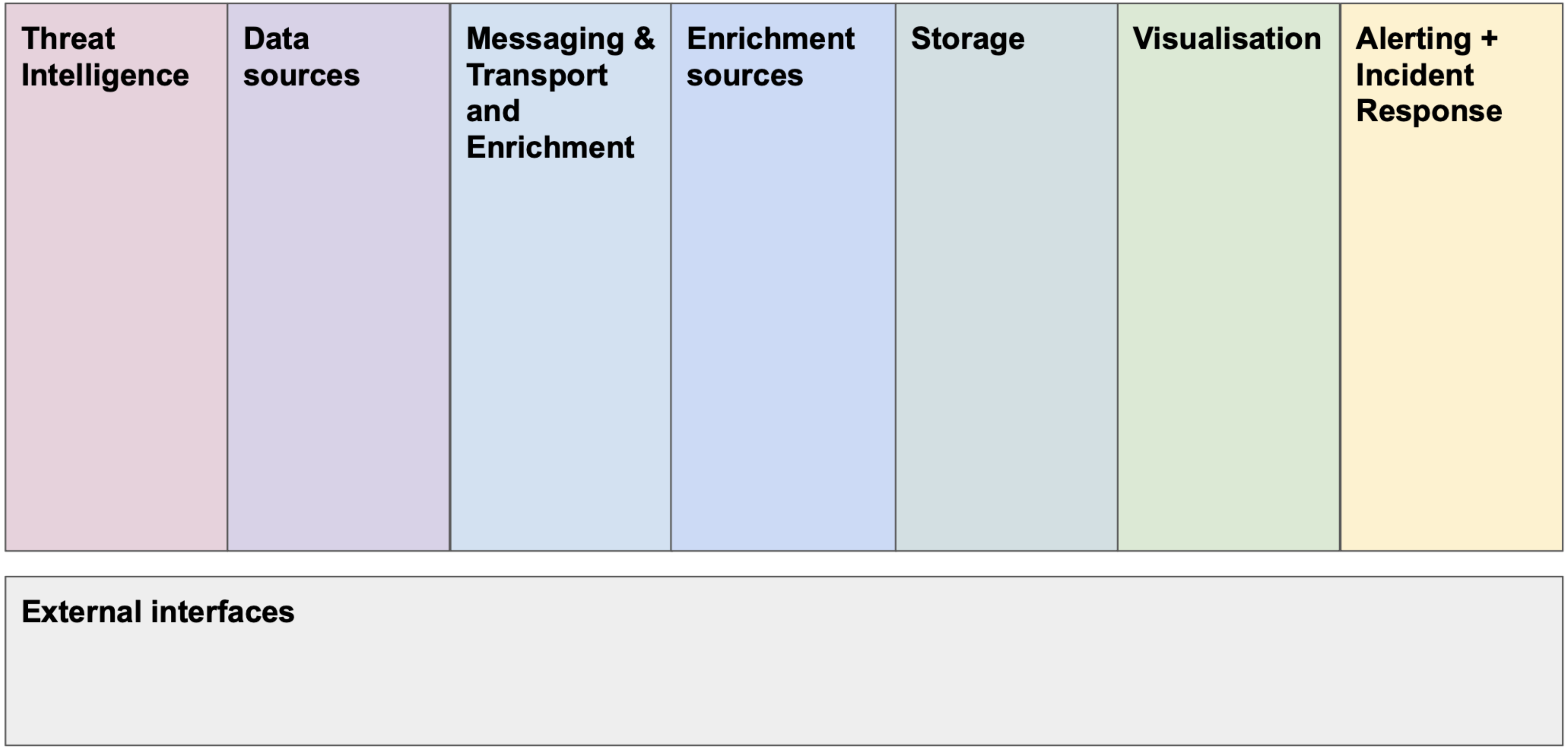
Having processes in place ensures a consistent approach to handling and preventing security incidents.

Tools are the protective shield against cyber threats. Tools and technology that are deployed correctly are the defense when no one else is watching.

Fermilab

[Let’s talk People and Process]

SOC Model



Threat Intelligence

Data sources

Messaging & Transport and Enrichment

Enrichment sources

Storage

Visualisation

Alerting + Incident Response

External interfaces

Collaborative Operational Security: The future of Cybersecurity for Research and Education

Next: Software intros

- Zeek
  - Fine grained network monitoring using deep packet inspection
- MISP
  - Threat intelligence sharing platform
- pDNSSOC
  - Lightweight SOC capability using a sensor in DNS infra coupled to threat intel source -> alerting