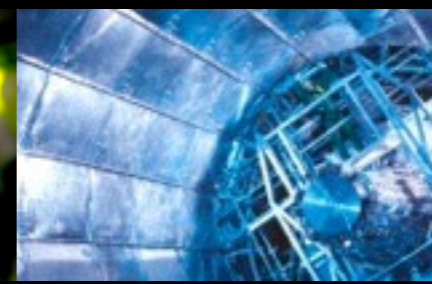
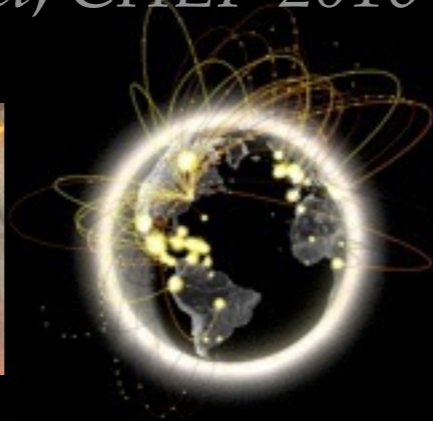


# The future of academic computing security

*Romain Wartel, CHEP 2016 Conference, San Francisco, October 8-14, 2016*





# Academic computing as a target

- Main targets are here to stay:
  - Money
    - Credit cards, financial applications, payroll systems, etc.
  - Computing resources
  - Any marketable asset
    - Identities, scientific data, medical records, online journals, etc.
- Main attackers profile:
  - Cybercriminals (money) — less opportunistic, more targeted
  - Hacktivists (delay, disrupt, destroy)
  - Nation-states (data, strategy, tender info, technology, IP)
- Data center infection vectors
  - SSH attacks or Linux privilege escalation more and more rare
  - Humans / identities
    - Phishing, malspam, drive-by downloads, phone calls, etc.

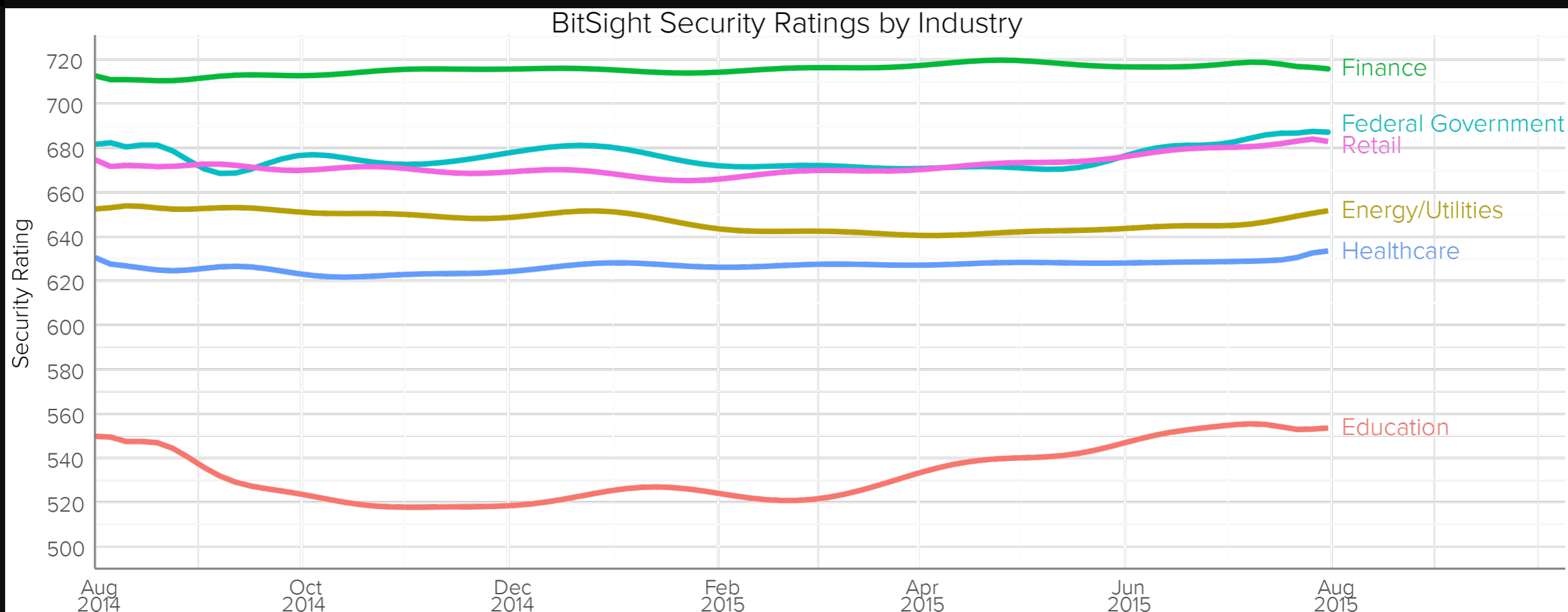


# MaaS + Affiliate model

- Malware-as-a-service : purchase/rent from vendor or broker
- Affiliate model: pay an affiliate to install your malware
- Affiliates usually concentrate on a specific market:
  - Affiliates may rent malware-as-a services or own techniques
  - Scope language and context
    - e.g. Dridex botnet ID 124 uses German and targets Swiss banks
  - Victims in relevant industry segment
    - e.g. do not infect “School, Academic, Data Center, Medicine, Cloud, Server, Anonymous, University, Nuclear, Hospital, Datacenter, Datacentre, Science, Government”
  - Hybrid: A given actor can use the same Word macro to spread a ransomware or banking trojan depending on geolocation



# Attacking academia as a business model



- **Academia is a viable market for cybercriminals**
  - Ransomware, finance fraud, etc.
  - Recently a large R&E institution agreed to pay ransomware
    - In a targeted (= not opportunistic) campus-wide attack
- **Offers a favorable cost/benefit ratio for many bad actors**

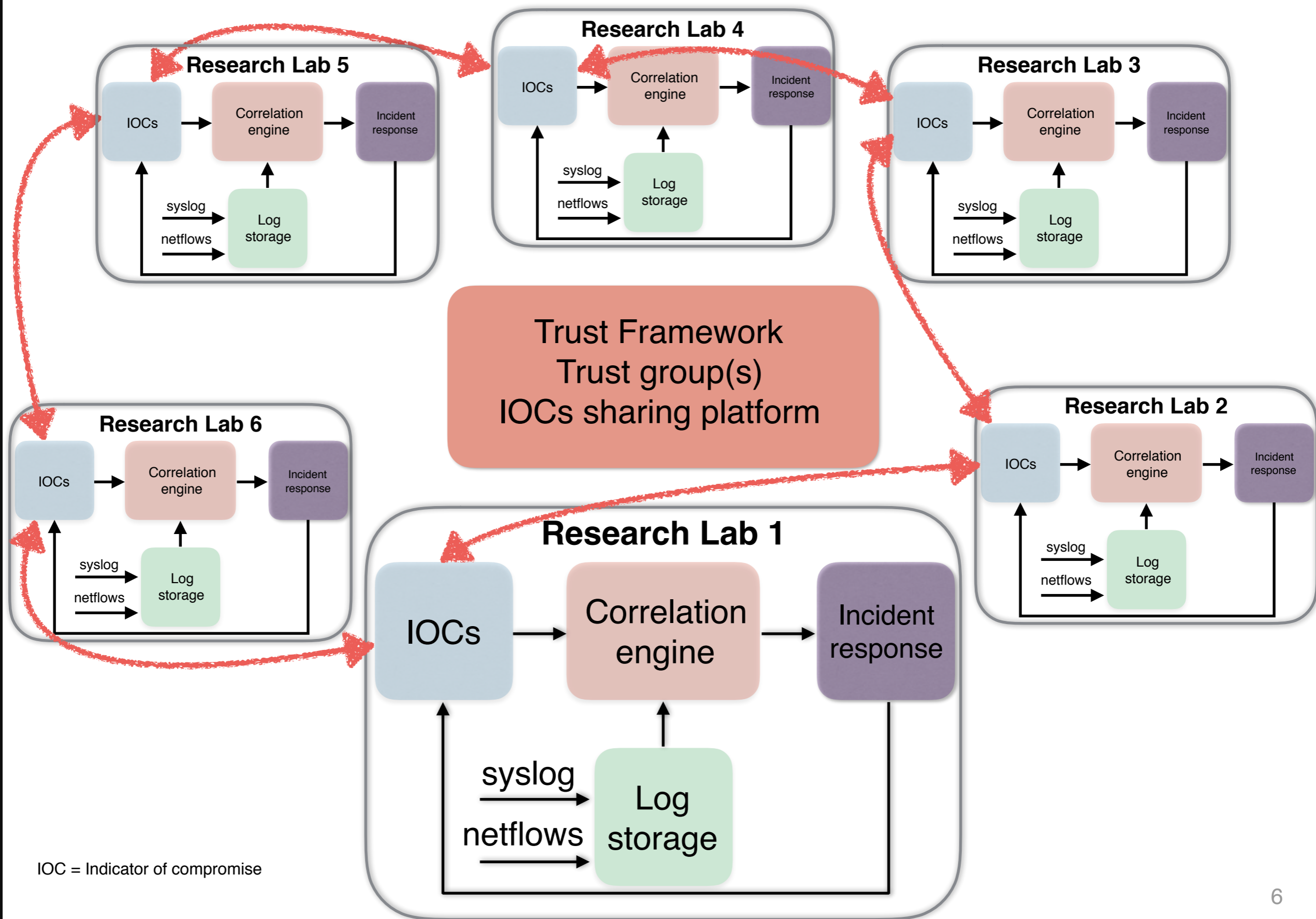


# Increasing costs, reducing benefits

- Academia needs to become less attractive to criminals:
  - Both increasing costs to attackers and reducing their benefits
- **Treat threat intelligence has a tradable commodity**
  - Give: Leverage your network of contacts and make it available  
Your assistance, a sinkhole or malware samples might be very valuable to others
  - Get: relevant intelligence, indicators of compromise, expertise
- Must become much more **efficient** regarding security
  - We already have a lot available, we could make better use of it!
- Campus security vs scientific computing
  - Scientific/grid/cloud security: project security, people, middleware
  - Campus security team: Visibility over network, email, Web, etc.
- **Crucial closely cooperate or merge operations**



# A global response



IOC = Indicator of compromise



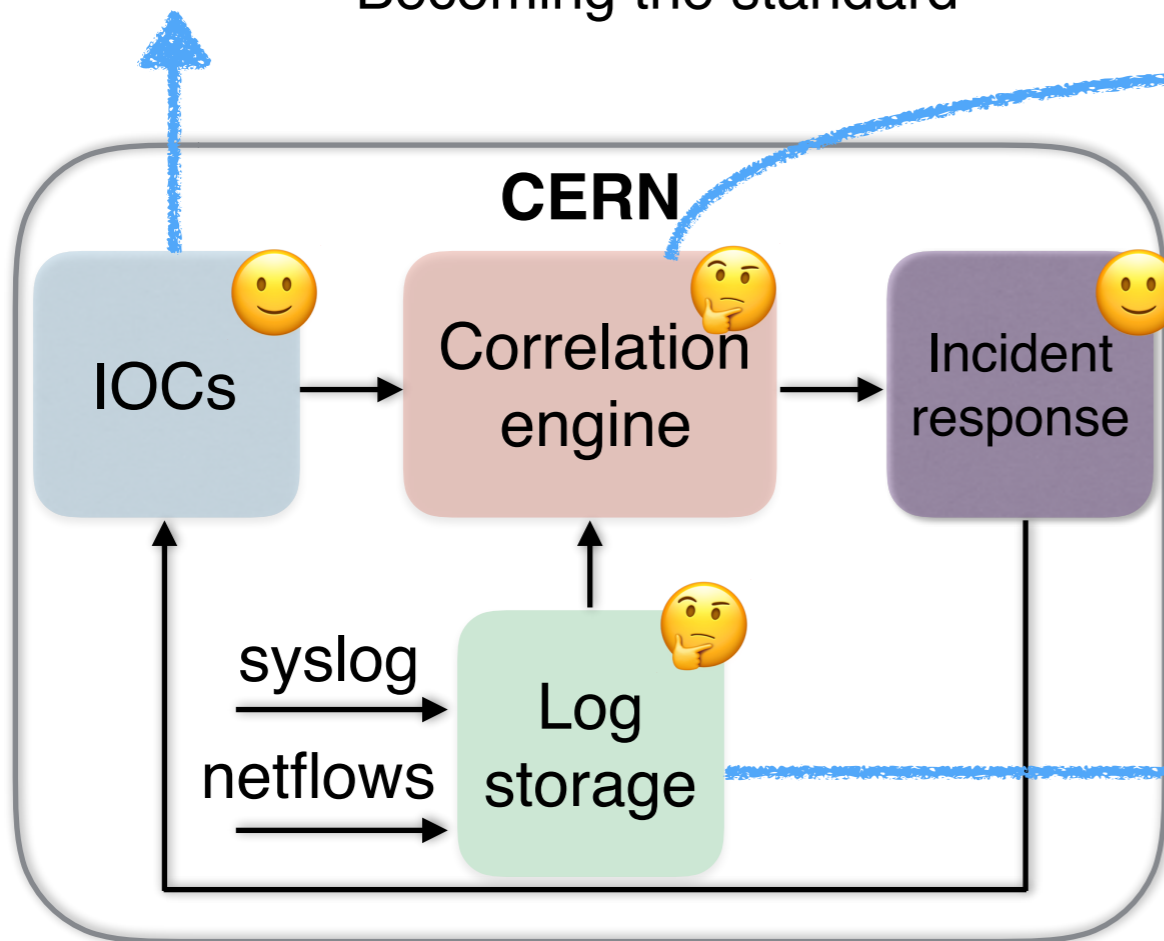
# SOC status at CERN



MISP:  
Happy with it  
Becoming the standard

Bro/Spark:

**Goal: 1 TB/day live IOCs correlation**  
(Bro: 250GB/day, Spark (550GB/day)  
New Bro release very promising  
Good deployment progress  
Correlation + network logs



HDFS/ElasticSearch:

**Goal: Storing 2 TB/day**  
**Retention goals:**  
- 3 months+ on ElasticSearch (real time index)  
- 1 year on HDFS (slower)

Slowly building production service

- Active engagement in several trust groups (IOCs)
- Collaboration and participation in the SOC WG
- Dedicated talk about Bro during HEPiX



# Conclusion

- Our community has to become more **efficient on security**
  - Engage with **trust framework** and threat **intelligence sharing**
  - Campus and grid/science/cloud security teams need to cooperate
- **Threat intelligence as a tradable commodity**
  - Our collaboration and network of contacts are precious assets
  - Our community needs assistance from private sector
- **Strategy: enable...**
  - Experienced/mature sites to get **access to IOCs** and to share back
  - Less resourced sites to **monitor/respond at a minimal cost**
  - Security teams to get logs, samples, setup sinkholes, etc.
- **Key challenges**
  - Highly heterogeneous security maturity + significant cultural gaps
  - Attacks against R&E are everyone's problem, but no one's responsibility...