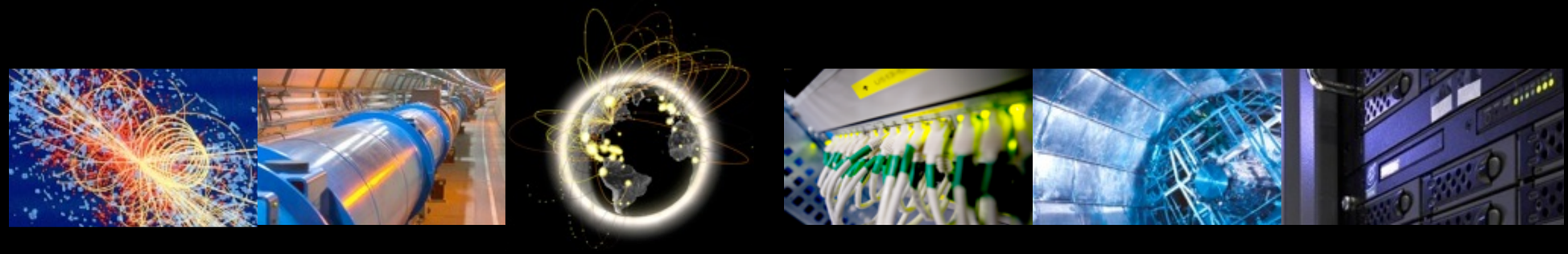
Security report



Romain Wartel, WLCG Grid Deployment Board, Taipei, 21st March 2018

WLCG
Worldwide LHC Computing Grid

CERN

Criminal skills vs WLCG

- Average attack way beyond skills of average WLCG site admin
  - Even for some basic, un-targeted attacks
  - Social engineering & vulnerabilities: endless infection vectors
  - Even advertisers are currently using malware-like domain generation algorithm (DGA)
  - Closely collaborating with your site(s) security team absolutely required

- Attackers:
  - Years of experiences
  - Evolved, modular malicious framework operated 24/7 over resilient infrastructures
  - No funding or staffing issue
  - Only need the victim to make one mistake or exploit a single vulnerability to succeed

- Get professional products, use frameworks and feed them indicators from friends

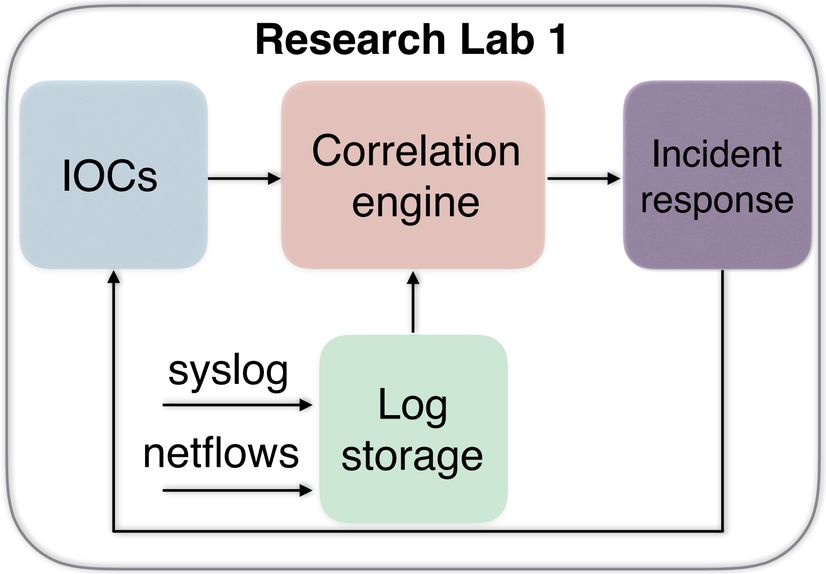
Your strategy in a nutshell

- You will not survive online alone.

- Attackers want your money, your resources, your personal and institution's data
  - Without external support, attackers will obtain all this.

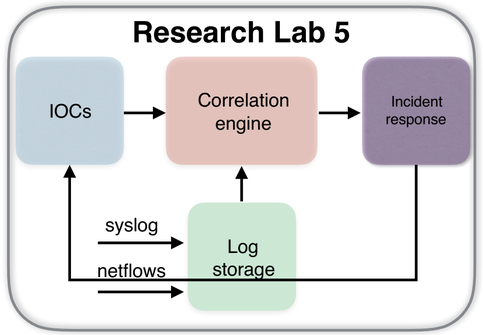
A community response

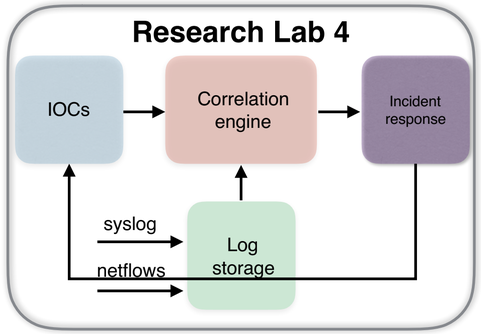
- Trust and collaboration –> Threat intelligence
- Crucial collaboration at each WLCG site:
  - Grid security contacts have the threat intelligence
  - Site security teams have access to the logs and network

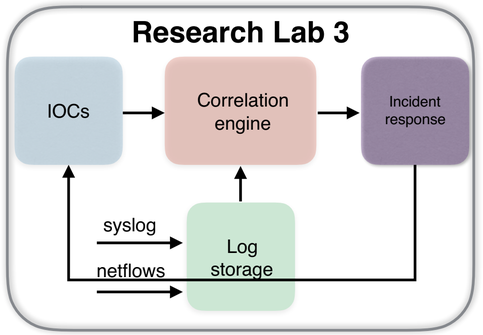


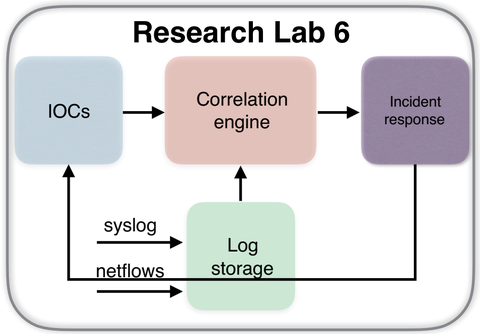
IOC = Indicator of compromise

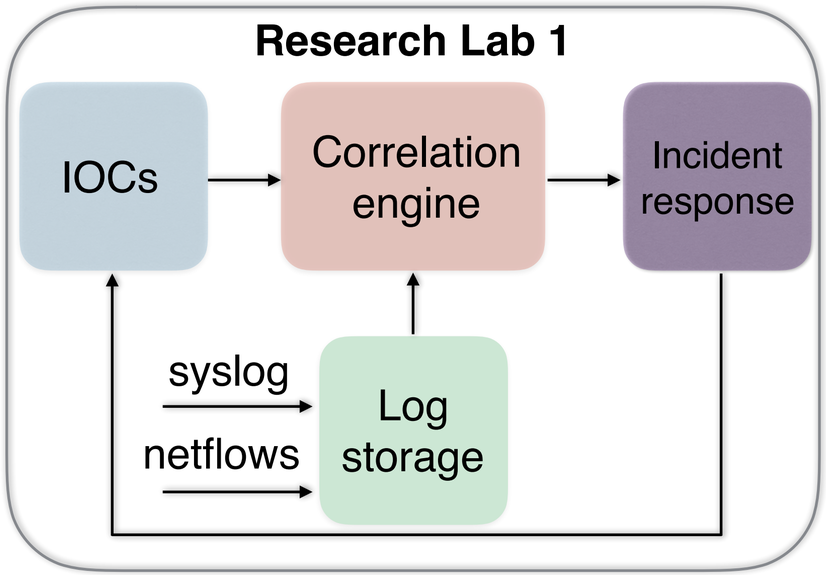
A community response

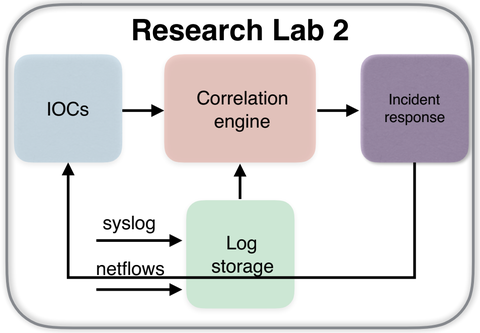






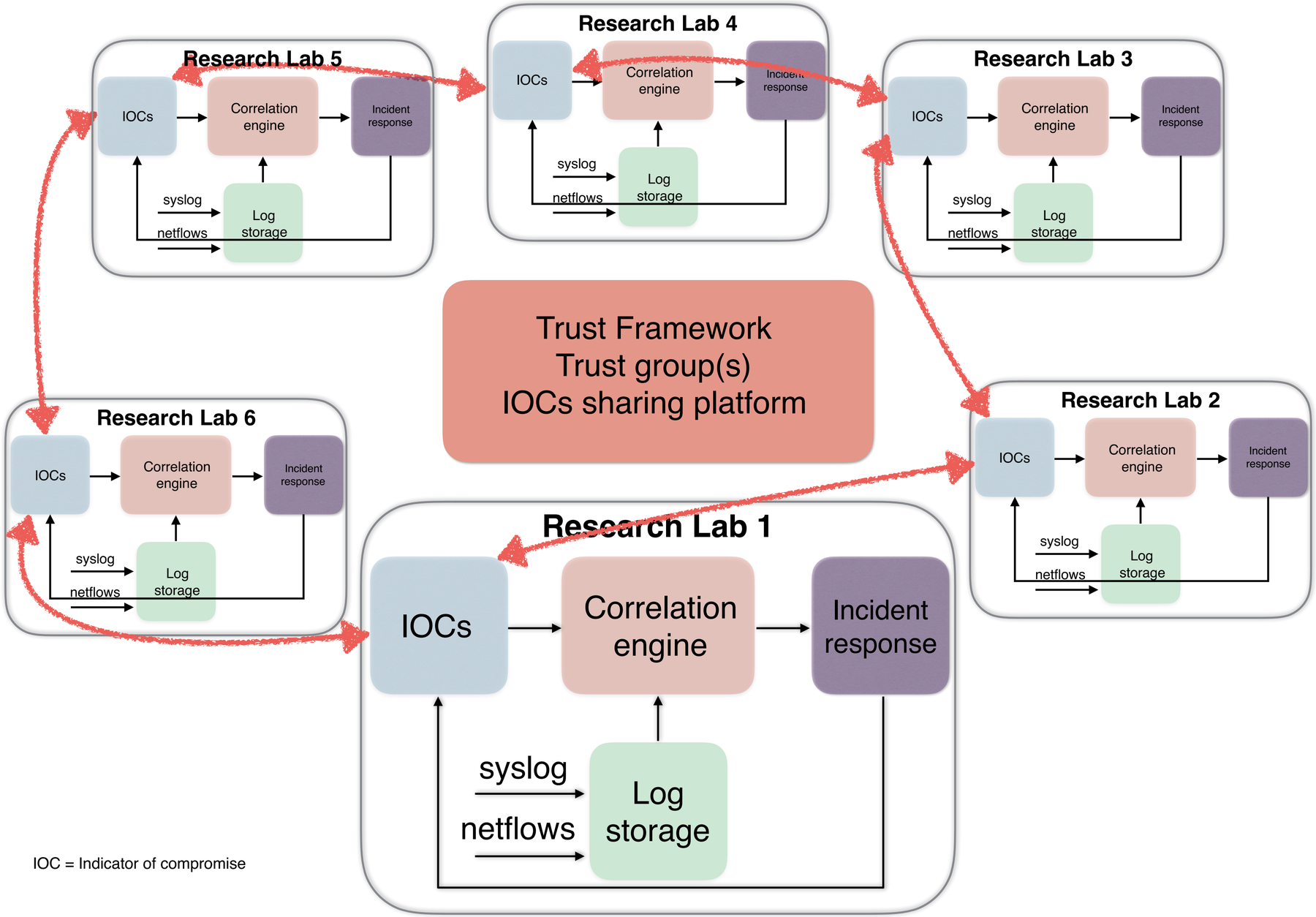






IOC = Indicator of compromise

A community response



IOC = Indicator of compromise

Proposed strategy for next 5 years

- Enable threat intelligence to be fully used by WLCG sites (See SOC WG)
  - Share quality threat intelligence among WLCG sites
  - Enable sites to receive and ACT on threat intelligence
- Convince site security teams to open up and collaborate
- Increase collaborations and build trust relationships (globally and locally)
  - Other infrastructures, local government CERTs, private vendors, etc.
- Assist WLCG sites in omplements appropriate SOC, IOCs and log correlation
  - WLCG has great working groups!
- Make security everyone's problem (and not a central team's full responsibility)
- Keep sites informed with malicious developments (GDB, vendors)
  - Improve site's security: email and desktop security, implement 2FA, « reinstall continuously »

Coming soon: Infrastructure compromises

- More IaaS and PaaS attacks (not just underlying hosts)
  - Result: full infrastructure compromises
- Necessary to design systems assuming complete compromise
  - Aim at eradicating persistence
  - Continuously re-install systems, verify configuration, keep up-to-date with security patches
  - Design, implement and operate forensics-friendly systems
    - IaaS, containers, elastic resources, etc. TRACEABILITY is paramount
  - Implement fined grained access control, limit privileges (to delay lateral movement)
  - Limit amount of personal/sensitive data stored, use second factor authentication
- Evolving paradigm:
  - 2000's: Operate secure services (protection)
  - 2010's: Operate defendable services (detection)
  - 2020's: Operate resilient services (recovery)

Key challenges in Asia

- Lack of technical expertise & high staff turn over in public sector
  - Training, training, training (in local language ideally!)
  - Interest usually limited 😕
- Culture
  - Different perception of risk and impact
  - The need for collaboration (local or international) not always perceived yet
  - Accepting (or admitting) weaknesses and communicating about them
  - Funding typically covers network configuration, but not operational security
- International collaborations
  - Politics often a difficulty: can be overcome at the technical level!
  - Langage is a big problem
- Many solutions possible… as long participants feel this address a need

Building a cohesive community

1. Identify like-minded organisations
2. Identify security or technical experts within them, or anyone willing to collaborate
3. Build trust relationships between participants
   (physical meeting, sharing war stories, etc.)
4. Establish common goals, needs and issues
5. Enable participants to share sensitive information (tools, mailing list)
6. Enable participants to act on intelligence… and share back!
7. Add value by pooling resources/effort (extra expertise for forensics, tools, etc.)
8. Establish strong external links with the of the security community
   (cross-membership, etc.)

How to encourage new members to join?

- The community can provide:
  - Free expertise, help, tools, tutorials, etc.
  - Indicators of compromise, experience from attacks

- New members can provide with no security expertise:
  - Contact points
  - Access to compromised machines
  - Data, log files

- As a new member, the bar is very low. But the benefits are high!
- Similar strategy when small trust groups aim at participating in global groups
  - Be pro-active, share what you have/can, build trust relationship, profit.

Chinese Security Federation

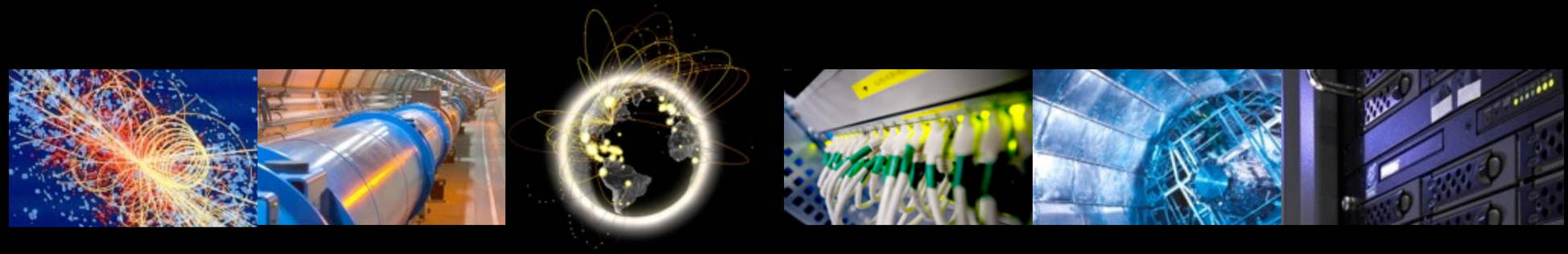
- Successful security training event at IHEP in October 2017
  - Mix of English and Chinese
  - Trainers from EU and US

Discussion

- How can we (WLCG) help improve further collaboration in ASIA?
  - Assist in creating trust groups?
  - Organise training events? (Do they really help? Do they need to be localised?)
  - Assist directly with security operations?

- Maybe a new operational security trust group could emerge from:
  - Asia Tier Forum? APGRIDPMA? APAN Security Working Group? PRAGMA?

Discussion



WLCG
Worldwide LHC Computing Grid