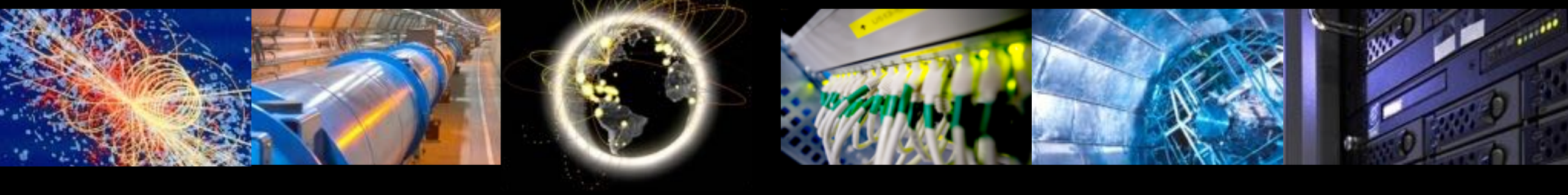
Security experience from WLCG

Romain Wartel, CERN-SKA Discussion, CERN, May 16th, 2017

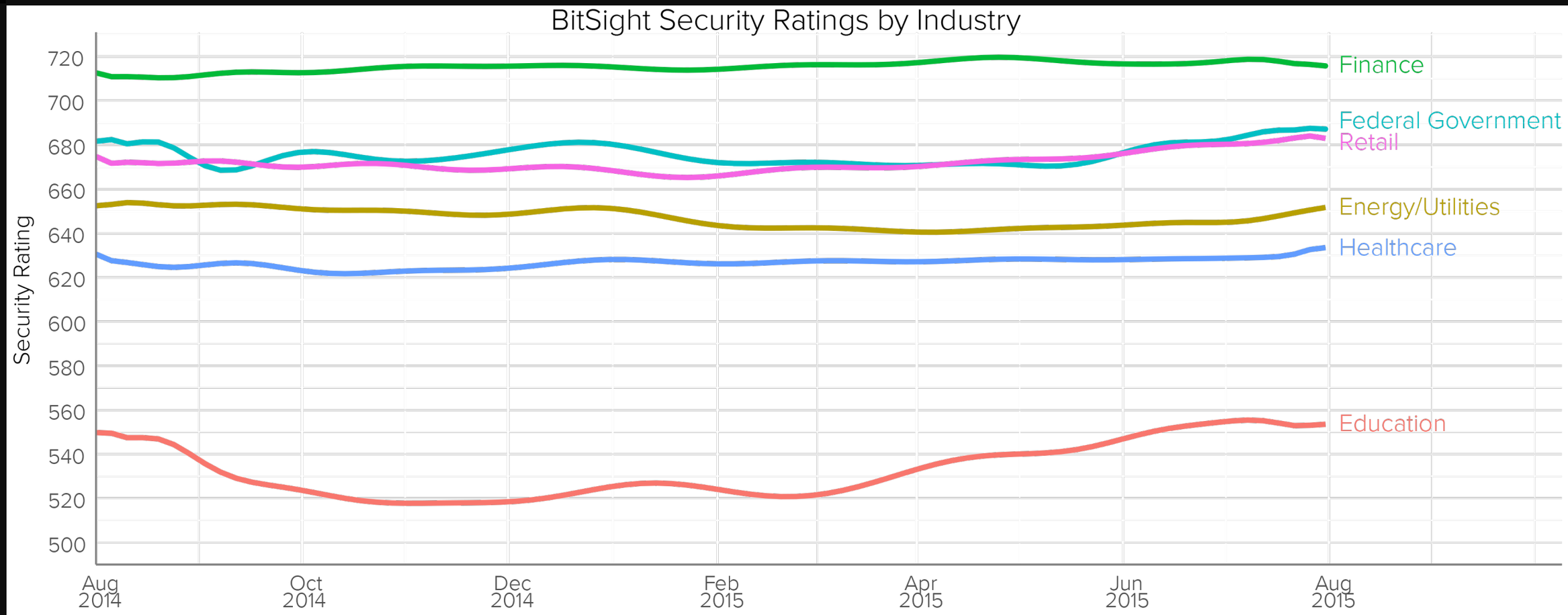


WLCG
Worldwide LHC Computing Grid

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.

Attacking academia as a business model



- Academia is a viable market for cybercriminals
  - Ransomware, finance fraud, etc.

Accesspay, Accountis, Accurate Reconciliation, ACE Software Solutions, ACI Money Transfer, ACI Worldwide, Adaptor Payments, agro-twin, Akshay Software, albany, Alliance Enterprise, Allied Engineering Group, Alliensoft, aptbacs, apt bacs, AvantGard Trax, Bacsactive-IP, BacscomIP, bacs-ip, bacstel-ip, bancline, bankline, BankTrade, BFK Service Bureau, bottomline, Broadridge, Cashbook IP, cashbook ltd, Clear2Pay, coconet, Connect-iP, crealogix, data interchange, Dion Global Solutions, direct corporate access, Direct Link, EastNets, EBICS, ECS Financials, elseware, episys quest, experian payments gateway, experian-payments-gateway, Finacle Payments, FinShare BPO, FinTRACE, FircoSoft, fisglobal, fis global, FIS Payment Gateway, fundtech, Global Payments System, Grange Bacstel-IP, grange IT limited, grange systems, Hyposwiss, IMS Payments, Infosys Ltd, ing bank nv, IntelliMatch, interbacs, Kyriba, Kyriba Application, luxtrust, macrogram, mammut soft, microgen, Micro Informatique, Misys Trade Portal, mosaic software, multicash, nCipher, omikron, Oracle Flexcube Universal Banking, PayBase, PayCentre, Process Performance for SWIFT, quatersoft, saa consultants, secure-ip, secure-ip, SironEmbargo, Smartstream Technologies, softcrew, Sopra Banking, Surecomp, TATA Consultancy Services, TCS BaNCS Payments, tellerplus, Tieto Payment Suite, TI Plus, TONBELLER, Tr8Star, TRADEWIZ International, ultra-aep, unified software, v1 limited, saa consultants, secure-ip, secure-ip, SironEmbargo, Smartstream Technologies, softcrew, Sopra Banking, Surecomp, TATA Consultancy Services, TCS BaNCS Payments, tellerplus, Tieto Payment Suite, TI Plus, TONBELLER, Tr8Star, TRADEWIZ International, ultra-aep, unified software, v1 limited, vocalink, Wallstreet Suite, wearev1, WebSeries, wpm education

- Offers a favorable cost/benefit ratio for many bad actors

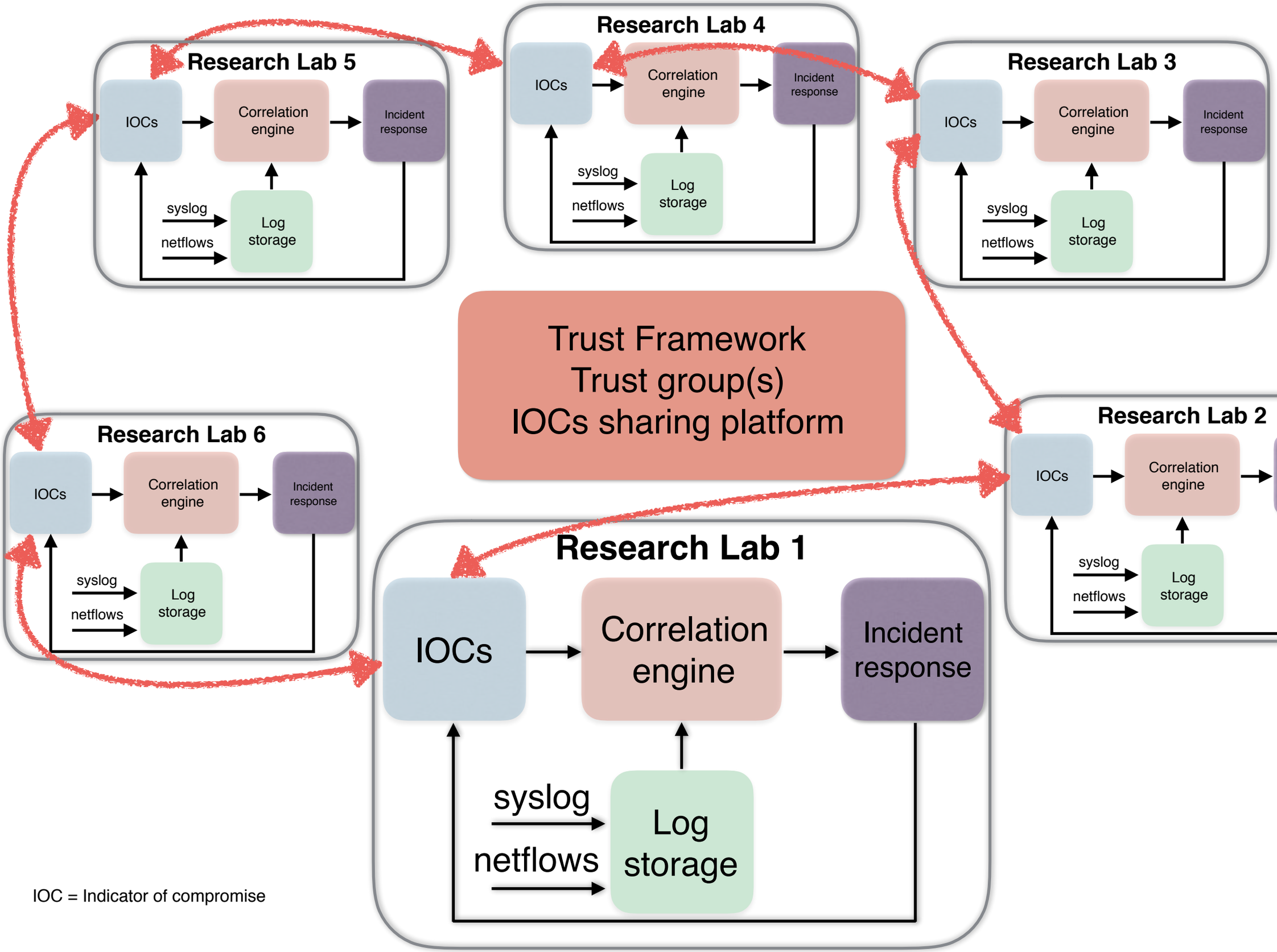
WLCG model

- Risk management
  - Opportunistic (for-profit)
  - APTs
- Operational security model
  - Incident response capabilities:
    contacts, procedure, expertise, controls
  - Campus vs scientific computing groups: danger!
  - Central vs distributed
- Main assets
  - A global collaboration on security
  - Protection others to protect us
  - Internet trust groups (LE, vendors)
  - Threat intelligence (from local to global)

WLCG model

- Policy and trust model
  - Per-project + inter-project
- Software model
  - Less control, more traceability
- Evaluating the maturity of your security status:
  - Do you have a plan/strategy/procedure to handle SKA-wide security incidents or intrusions? If so, does it foresee central coordination capabilities?
  - Do you have plans to collect/leverage/share threat intelligence among the different organizations participating in SKA?
  - Do you share operational security details or threat intelligence with peer projects outside SKA? With the private sector?
- FIM considerations (credits: Hannah Short)
  https://docs.google.com/document/d/13BoVSTnKPZF961ho1M_Tk5kHzRGct-Oo024Y5IYVfJQ/view

A global response



IOC = Indicator of compromise