USING BRO FOR OPERATIONAL SECURITY IN DISTRIBUTED COMPUTING: WLCG SECURITY OPERATIONS CENTER WG

LIVIU VÂLSAN, DAVID CROOKS

BRO WORKSHOP EUROPE, 18TH OF SEPTEMBER 2018

WLCG: WORLDWIDE LHC COMPUTING GRID

- Global collaboration linking up national and international grid infrastructures
  - More than 170 computing centres in 42 countries

- Providing global computing resources to store, distribute and analyse data from the Large Hadron Collider (LHC) at CERN
  - Fundamental research – particle physics
  - 50 – 70 Petabytes of data / year

WORKING GROUP BACKGROUND

- Inside WLCG there is a need to monitor cluster environment in a new context which can include virtualised / containerised systems
- Potentially more opaque than existing grid systems
- Network monitoring key to understanding cluster state

SECURITY OPERATIONS CENTER

- Gather relevant security monitoring data from different sources
- Aggregate, enrich and analyse that data for use in the detection of security events and any subsequent actions
- A SOC consists of a set of software tools and the processes connecting them

WORKING GROUP STRATEGY

- Identify key components required for a minimum viable product SOC which can then be built on

- Answer two questions
  - What is happening in a given cluster?
  - What events are taking place that we need to care about? (internally or externally)

WORKING GROUP STRATEGY

- Network monitoring
  - Intrusion Detection System: Bro

- Threat Intelligence
  - Malware Information Sharing Platform (MISP)
    - Develop trust frameworks to share threat intelligence

WORKSHOPS

- Became clear that a useful way of making progress with this technical work is through face to face workshops

- December 2017
  - Initial deployment

- June 2018
  - Further in-depth work on key topics

WORKSHOPS: DECEMBER 2017

- The first WLCG SOC WG Workshop in 2017 focused on the initial deployment of the MISP and Bro components
  - Documentation
  - Puppet modules + CERN built RPMs
  - Sync with WLCG MISP instance hosted at CERN

WORKSHOPS: JUNE 2018

- The second workshop in June 2018 gave more time to specific areas of interest:
  - Network topologies including tapping and mirroring
  - Data ingestion and visualisation
  - Advanced aggregation and correlation of alerts
  - Incident Response and MISP configuration

WORKSHOPS: JUNE 2018 - KEY OUTCOMES

- Importance of tuning for Bro configuration
- Need for validation of deployment
  - Local and wider scope

- Feedback towards structure of future workshops

OUTCOMES

- Technology stack
  - Pursued through workshops and regular meetings

- Social and political cultural shift in sharing of intelligence
  - Essential component is collaboration between grid and site security teams
  - Sharing experience through case studies

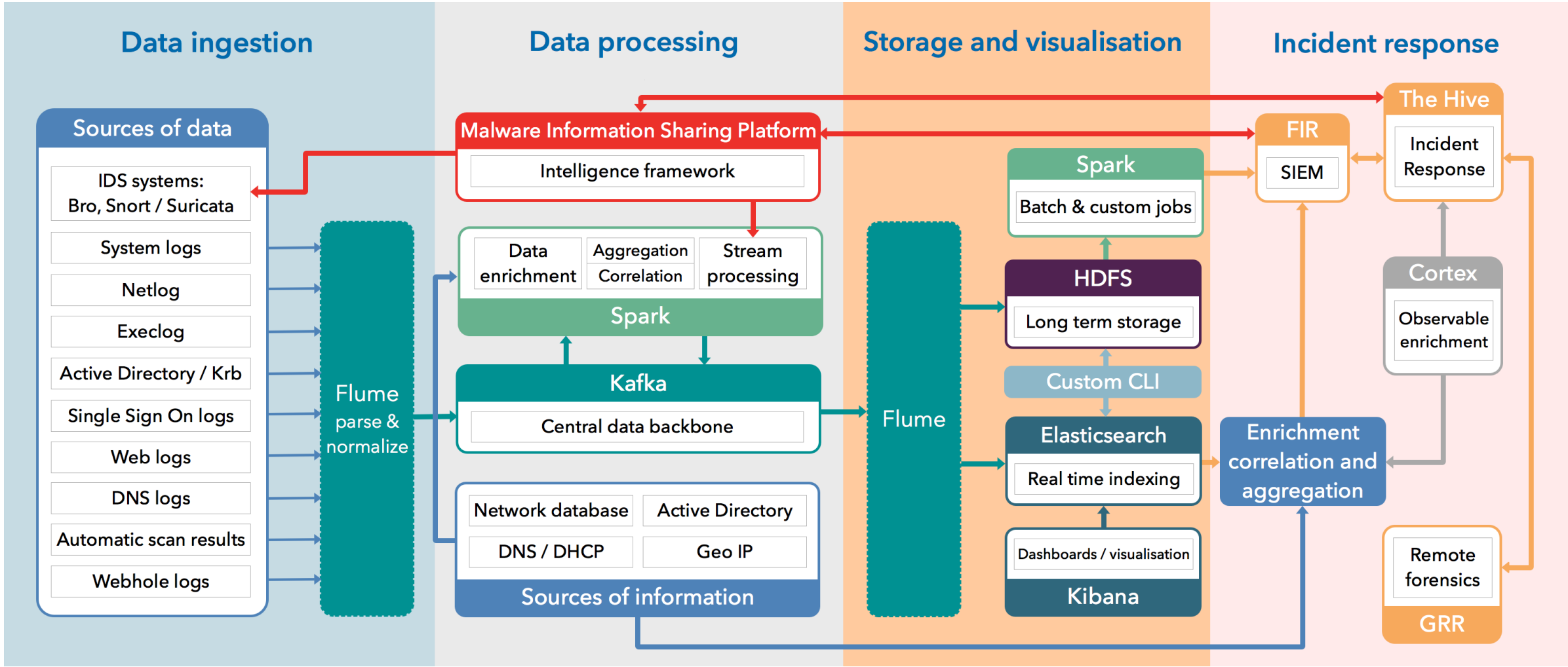
NEXT STEPS FOR THE WLCG SOC WORKING GROUP

- Continue deployment of components at a range of sites
- Build out deployment strategy
  - Add validation steps (locally and on a wider scale)
  - Add other SOC components gradually
- Continue trust group discussions

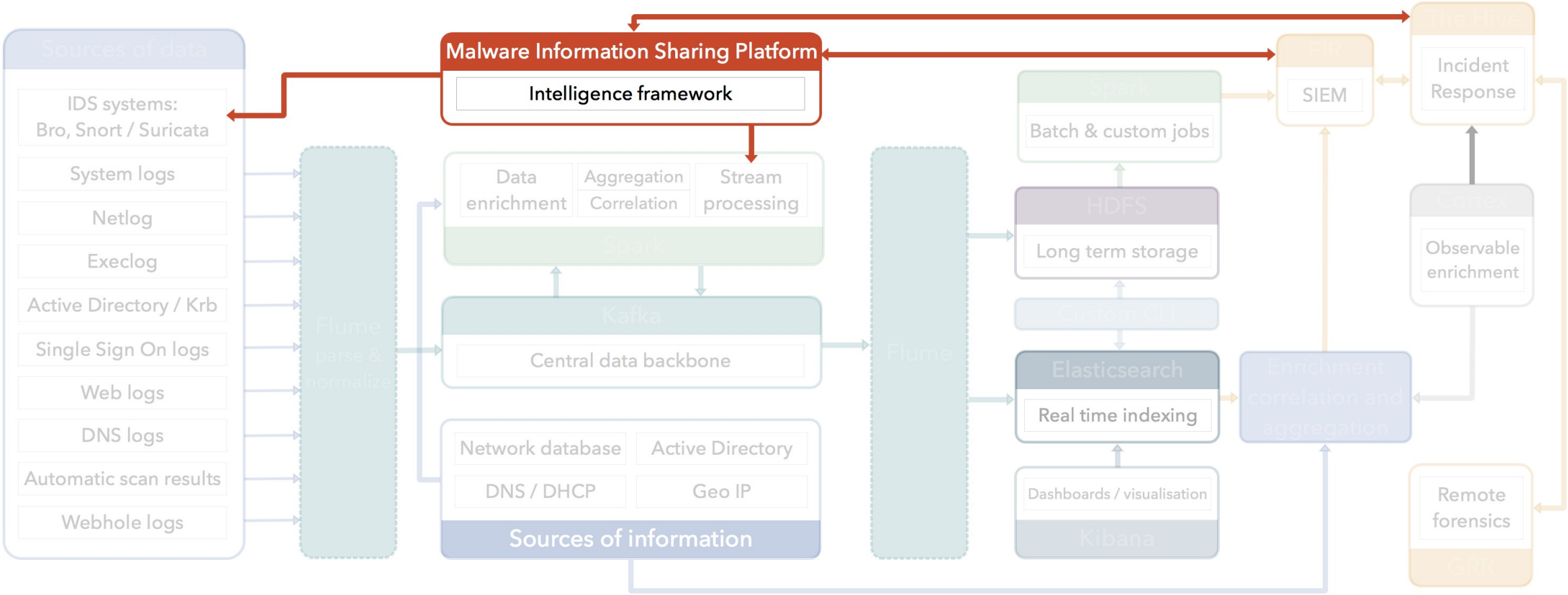
European Organization for Particle Physics

Exploring the frontiers of knowledge

SYSTEM ARCHITECTURE OF THE CERN SOC



THREAT INTELLIGENCE



THREAT INTELLIGENCE

- Malware Information Sharing Platform (MISP) as the sole threat intelligence platform at CERN
  - Automatic sharing of intelligence data with trusted peers

- CERN is currently operating 3 different instances:
  - Main CERN instance (~ 750 000 IoCs)
  - Worldwide LHC Computing Grid (WLCG) central MISP instance (~ 375 000 IoCs)
  - Development MISP instance used for MISP development (CERN is an active contributor) and for validating new MISP releases

THREAT INTELLIGENCE: SECURITY EVENTS

My Events | Org Events | Filter

Published	Source org	Member org	Id	Clusters	Tags	#Attr.	#Corr.	Email	Date	Info	Distribution	Actions
✔	[redacted]	[redacted]	8900		tlp:white circl:incident-classification="malware"	2		cert-ioc@cern.ch	2018-03-07	URL delivering crypto miner	All	
✔	[redacted]	[redacted]	8895		ecsirt:malicious-code="worm" malware_classification:malware-category="Downloader" malware_classification:malware-category="Worm" tlp:green LDO-CERT:detection="toSIEM"	0		cert-ioc@cern.ch	2018-03-06	Campaign Malspam "Richiesta" (request) - Unknown malware	All	
✔	[redacted]	[redacted]	8899	Tool: Emotet	tlp:green	4		cert-ioc@cern.ch	2018-03-02	Malspam "New Bankofamerica payment notice"	All	
✔	[redacted]	[redacted]	8898		tlp:green	4		cert-ioc@cern.ch	2018-03-02	Malspam "Przeterminowane płatności / PBS Connect Polska Sp. z o.o."	All	
✔	[redacted]	[redacted]	8897		circl:incident-classification="malware" osint:source-type="blog-post" tlp:white	53	1	cert-ioc@cern.ch	2018-03-06	Malware "TSCookie"	All	
✔	[redacted]	[redacted]	8896		Phishing enisa:nefarious-activity-abuse="phishing-attacks" circl:incident-classification="phishing"	9		cert-ioc@cern.ch	2018-03-06	British Telecom Phishing	All	
✔	[redacted]	[redacted]	8890		Phishing enisa:nefarious-activity-abuse="phishing-attacks" circl:incident-classification="phishing"	5		cert-ioc@cern.ch	2018-03-05	Orange France Phishing	All	
✔	[redacted]	[redacted]	8875		tlp:green circl:incident-classification="phishing" ecsirt:fraud="phishing" osint:source-type="pastie-website"	91		cert-ioc@cern.ch	2018-03-02	Phishing and Malware URL's	All	
✔	[redacted]	[redacted]	8892		Gozi tlp:green tlp:amber	7		cert-ioc@cern.ch	2018-03-06	Gozi campaign (2018-03-06)	Organisation	
✔	[redacted]	[redacted]	8893		tlp:green Retefe	26		cert-ioc@cern.ch	2018-03-06	Retefe Spam Run (2018-03-06 - Psychopate Gewalttäter. Beschreibung Information. Strasse NR)	Organisation	
✔	[redacted]	[redacted]	8894		tlp:white malware:Pony	17	1	cert-ioc@cern.ch	2018-03-06	Pony malspam campaign	All	
✔	[redacted]	[redacted]	4874	Ransomware: Locky	tlp:white	49	22	liviu.valsan@cern.ch	2016-12-20	Locky 2016-12-20 : Affid=3, DGA=556677 - "for printing" - "Certificate_123456.xls"	All	
✔	[redacted]	[redacted]	8891		tlp:white Locky QuantLoader Threat:Ransomware	26	5	cert-ioc@cern.ch	2018-03-05	Locky - NemuCod - QuantLoader malspam campaign	All	
✔	[redacted]	[redacted]	8869	Tool: Emotet	tlp:white ncsc-nl-ndn:feed="generic"	35	1	cert-ioc@cern.ch	2018-03-02	EMOTET Malspam	All	
✔	[redacted]	[redacted]	8889	Tool: Emotet Attack Pattern: PowerShell Obfuscated Files or Information Preventive Measure: Block Macros Course of Action: PowerShell Mitigation Connection Proxy Mitigation	CTI :: Confidence :: High veris:action:malware:variety="Exploit vuln" veris:action:malware:vector="Email link" veris:actor:motive="Financial" veris:action:malware:variety="Capture app data" veris:action:social:variety="Phishing"	36		cert-ioc@cern.ch	2018-03-05	Emotet detected: hxxp://skovlunden.com/Invoices-Overdue/	All	
✔	[redacted]	[redacted]	8881		tlp:white	7		cert-ioc@cern.ch	2018-03-04	Crypto miner	All	

THREAT INTELLIGENCE: INDICATORS OF COMPROMISE

Malicious Bash Script

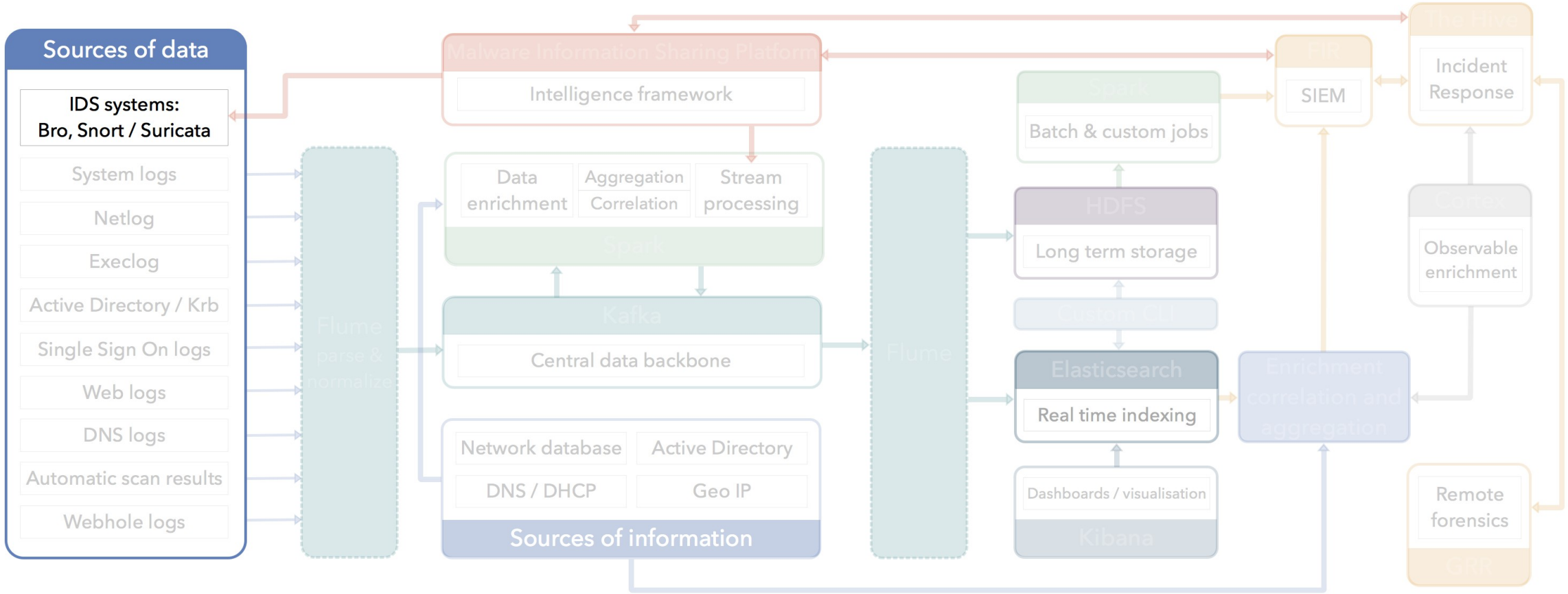
Event ID	8887
Uuid	5a9d1aa2-16c4-4100-8d44-0037ac130003
Source Organisation	[redacted]
Member Organisation	CERN
Contributors	
Email	cert-ioc@cern.ch
Tags	tlp:white x circl:incident-classification="malware" x malware_classification:malware-category="Trojan" x circl:incident-classification="system-compromise" x +
Date	2018-03-05
Threat Level	Low
Analysis	Ongoing
Distribution	All communities
Info	Malicious Bash Script
Published	Yes
#Attributes	12
Sightings	0 (0) - restricted to own organisation only.
Activity	

Pivots | Galaxy | Attributes | Discussion

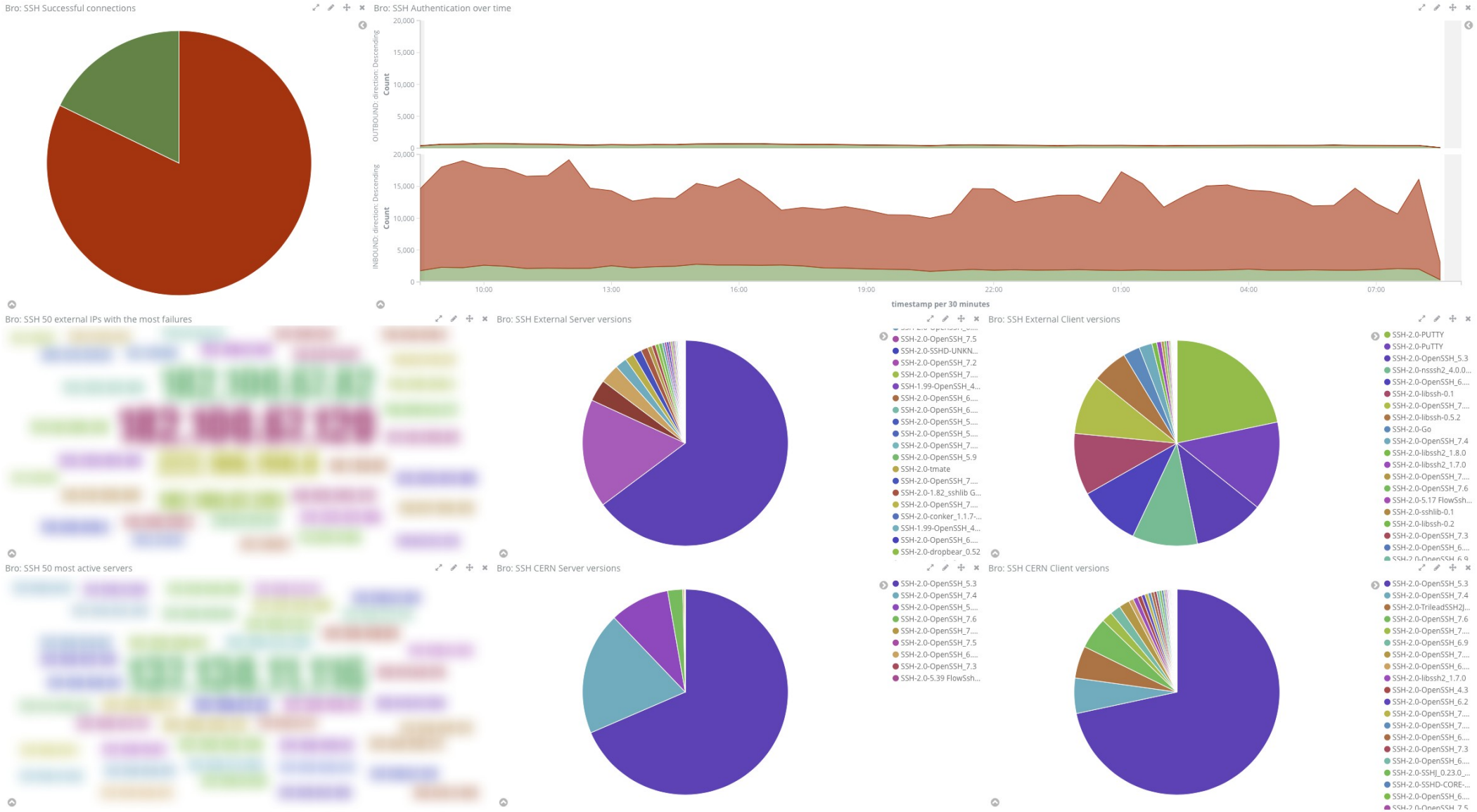
Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2018-03-05		Artifacts dropped	filename|sha256	minerd 2d89b48ed09e68b1a228e08fd66508d349303f7dc5a0c26aa5144f69c65ce2f2			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Artifacts dropped	filename|sha256	transfer.sh 615f70c80567aab97827f1a0690987061e105f004fbc6ed8db8ebee0cca59113			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Artifacts dropped	filename|sha256	unixinfect.tar.gz f14d021a26479c6d2592142009d0cf6731c91438a672dbd7a4f5a9829e377c15			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Artifacts dropped	pattern-in-file	AAAAB3NzaC1yc2EAAAADAQABAAABAQDV1VxPVZFUOOWZwMFVBwP/904lhAZNj2U5DPsZylWw33jHeFREIM++XnUYmkMDiu8KuJXnFDJMkyXxsq77fOpDhVGOoexII3+P6SmZWVlWwnhOgvxhccgT72J+LPZEIwPqPZQVHR4ksdVSnMVreyZs+rQ7O+L2xychpqzelrk4Q/08f5XreOnq4Rgxp9oKwSlf7vKmQ7tUWUxfMHHL1wQYZPmdKpgSi/JmokLpp5cKAT7r0gGOj1jV8ZAJc+z45Ts2JBH9JYscHBssh7MBWWymcjXANd9a6XaQnbnI6nOFFNyYm8dBuLkGpEUNCdMq/jc5YLfnAnbGVbBMhuWzaWUp		SSH Key	✓			Yes	Inherit	(0/0/0)		
2018-03-05		Artifacts dropped	filename|sha256	glibc-2.14.tar.gz 18d9a0296260fd9529d59229c1dcb130ee8a18a1dd71c23712c39056cc0eb0b3			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Artifacts dropped	filename|sha256	clay 260ef4f1bb0e26915a898745be873373f083227a4f996731f9a3885397a49e79			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Network activity	domain|ip	xksqu4mj.fri3nds.in 185.10.68.202			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Payload delivery	url	http://xksqu4mj.fri3nds.in/tools/clay			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Payload delivery	url	http://xksqu4mj.fri3nds.in/tools/minerd			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Payload delivery	url	http://xksqu4mj.fri3nds.in/tools/glibc-2.14.tar.gz			✓			Yes	Inherit	(0/0/0)		
2018-03-05		Payload delivery	url	http://xksqu4mj.fri3nds.in/tools/transfer.sh			✓			Yes	Inherit	(0/0/0)		

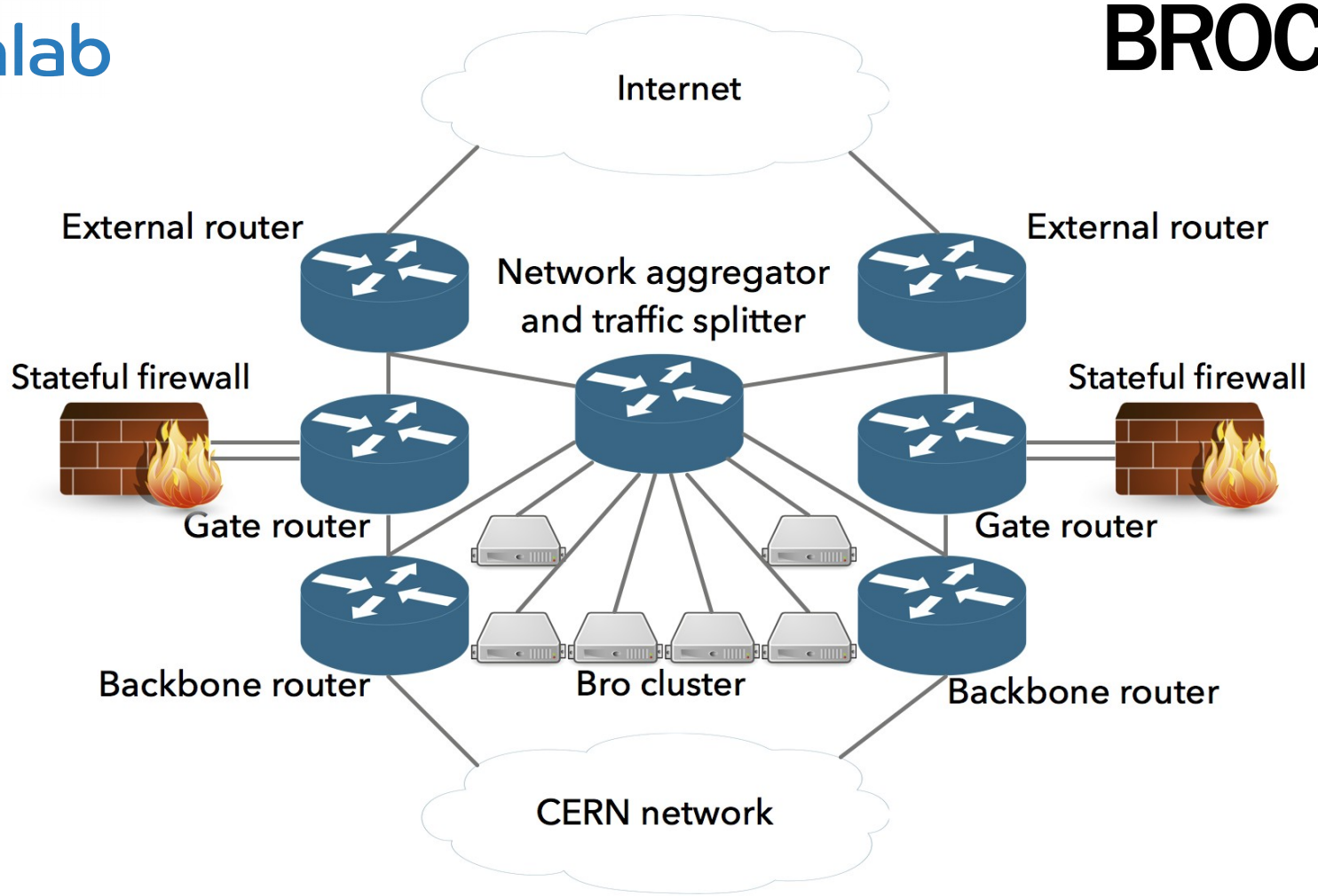
NETWORK BASED INTRUSION DETECTION



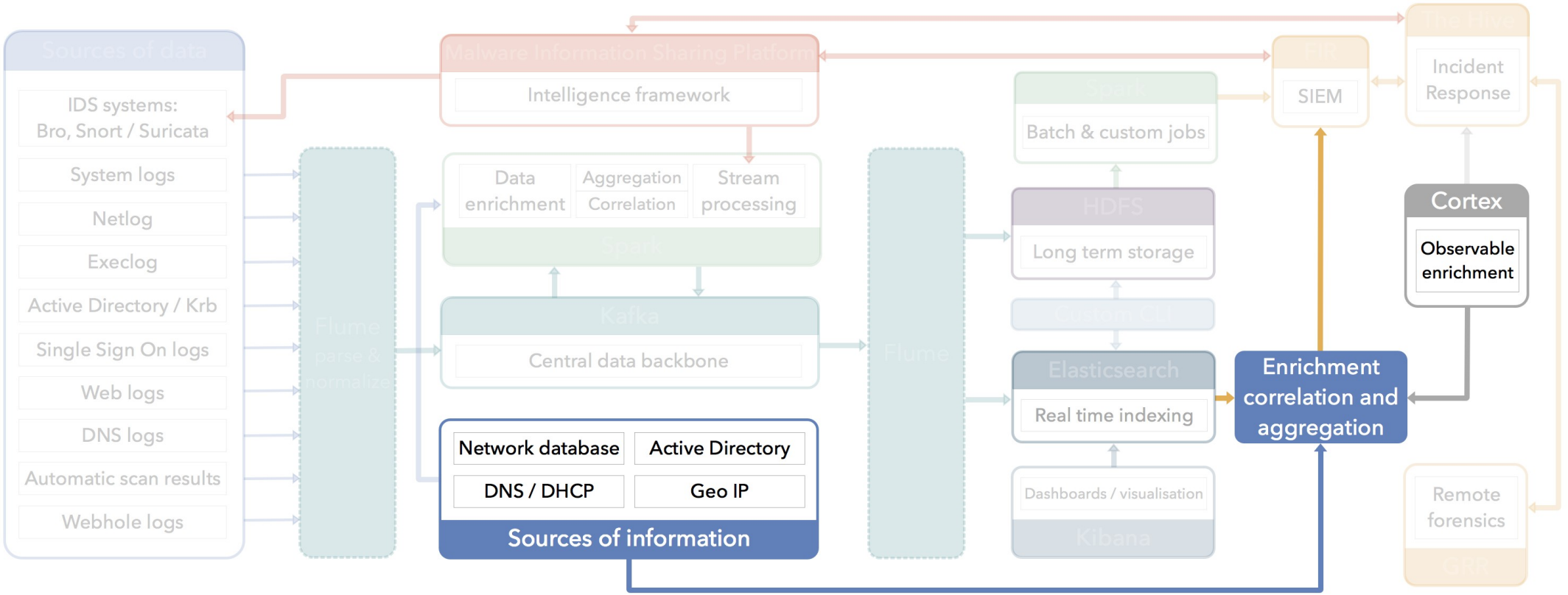
BRO IDS: SSH TRAFFIC



NETWORK TRAFFIC AGGREGATOR AND SPLITTER



ADVANCED PROCESSING OF NOTIFICATIONS

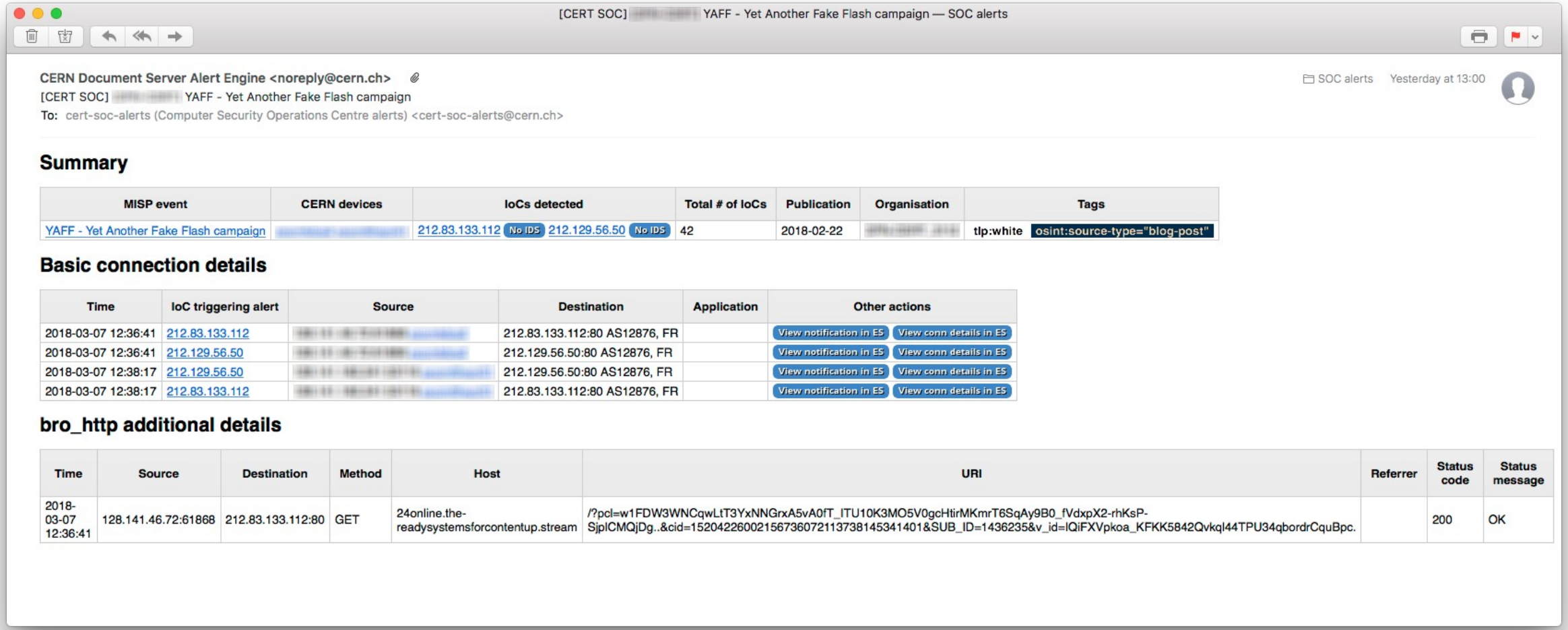


ADVANCED PROCESSING OF NOTIFICATIONS

- Advanced aggregation & correlation
- Additional enrichment of data
  - Only for logs linked to alerts
  - 100% accurate

- Output used by the Computer Security team for user notifications and follow-up

ADVANCED PROCESSING OF NOTIFICATIONS



[CERT SOC] YAFF - Yet Another Fake Flash campaign — SOC alerts

CERN Document Server Alert Engine <noreply@cern.ch>
[CERT SOC] YAFF - Yet Another Fake Flash campaign
To: cert-soc-alerts (Computer Security Operations Centre alerts) <cert-soc-alerts@cern.ch>

SOC alerts Yesterday at 13:00

Summary

MISP event	CERN devices	IoCs detected	Total # of IoCs	Publication	Organisation	Tags
YAFF - Yet Another Fake Flash campaign		212.83.133.112 No IDS 212.129.56.50 No IDS	42	2018-02-22		tlp:white osint:source-type="blog-post"

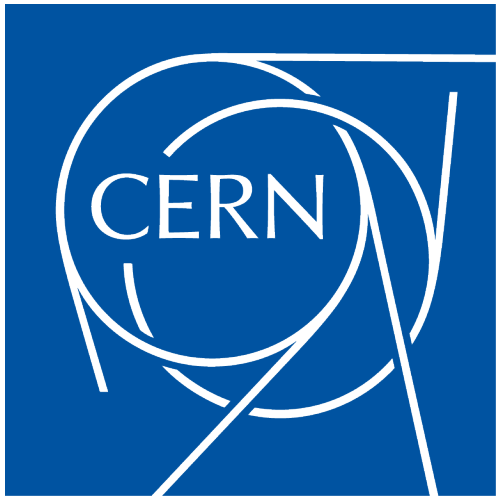
Basic connection details

Time	IoC triggering alert	Source	Destination	Application	Other actions
2018-03-07 12:36:41	212.83.133.112		212.83.133.112:80 AS12876, FR		View notification in ES View conn details in ES
2018-03-07 12:36:41	212.129.56.50		212.129.56.50:80 AS12876, FR		View notification in ES View conn details in ES
2018-03-07 12:38:17	212.129.56.50		212.129.56.50:80 AS12876, FR		View notification in ES View conn details in ES
2018-03-07 12:38:17	212.83.133.112		212.83.133.112:80 AS12876, FR		View notification in ES View conn details in ES

bro_http additional details

Time	Source	Destination	Method	Host	URI	Referrer	Status code	Status message
2018-03-07 12:36:41	128.141.46.72:61868	212.83.133.112:80	GET	24online.the-readysystemsforcontentup.stream	/?pcl=w1FDW3WNCqwLtT3YxNNGrxA5vA0fT_ITU10K3MO5V0gcHtirMKmrT6SqAy9B0_fVdxpX2-rhKsP-SjplCMQjDg..&cid=152042260021567360721137381453414 01&SUB_ID=1436235&v_id=lQiFXVpkoa_KFKK5842Qvkql44TPU34qbordrCquBpc.		200	OK


WLCG
Worldwide LHC Computing Grid


CERN