CERN

European Organization for Particle Physics

Exploring the frontiers of knowledge

DESIGNING A LARGE-SCALE SECURITY OPERATIONS CENTRE

CERN-CNAF COMPUTER SECURITY SEMINARS, 8TH OF JULY 2020

LIVIU VÂLSAN, ON BEHALF OF THE CERN COMPUTER SECURITY TEAM

WHAT IS A SECURITY OPERATIONS CENTER?

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

- Ensures that security incidents are properly:
  - Identified
  - Analysed (real time and historical data)
  - Reported
  - Acted upon

SYSTEM DESIGN

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

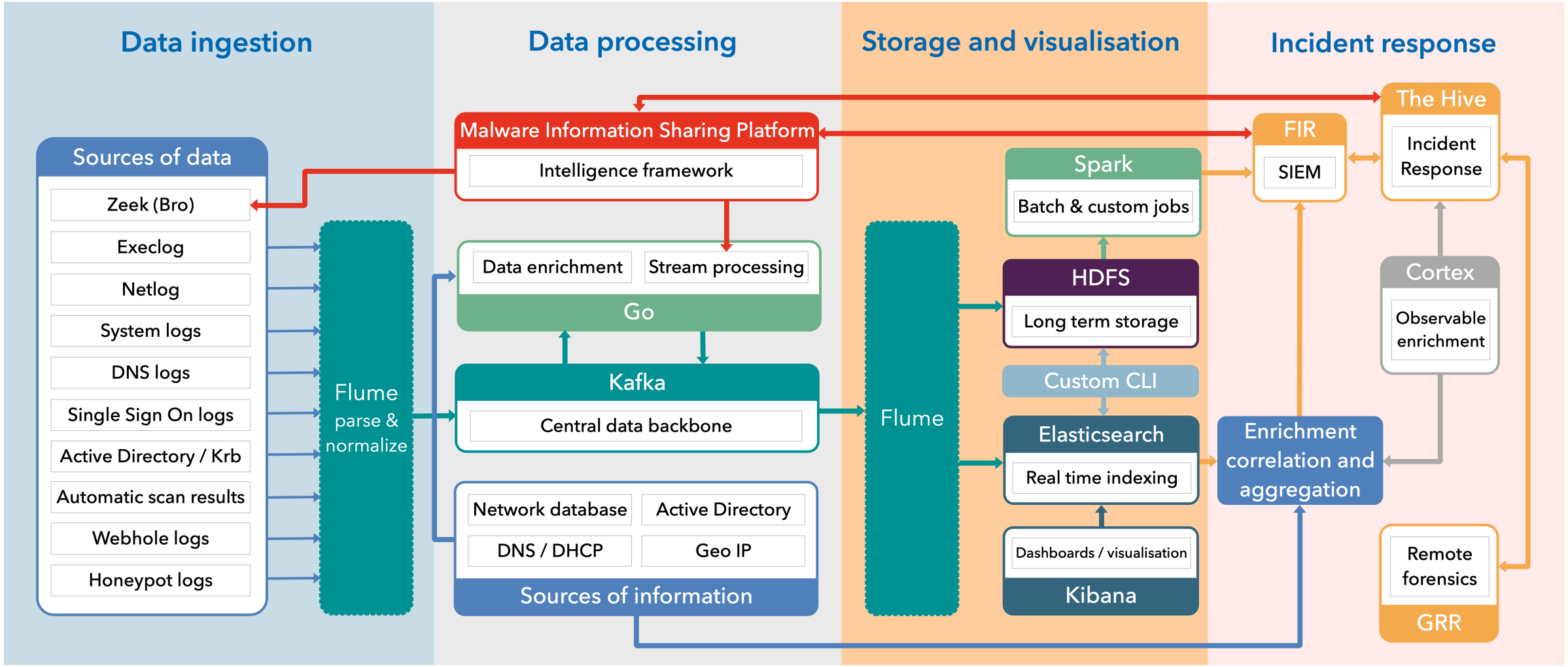
TECHNOLOGY GOALS

- Scale out, not scale up
- Integrated with the rest of the CERN IT ecosystem
- Use of commodity hardware (as much as possible)
- Use of cheap, massively-scalable storage (standard disk arrays)
- Deployment inside OpenStack (whenever possible)
- Configuration management done via Puppet

PRIVACY/SECURITY CONCERNS

- Every component follows strong security requirements:
  - Data transfers encrypted
    - Using TLS
  - Authentication used for all data accesses
    - Mostly Kerberos, password for Elasticsearch
  - Authorization & ACLs
    - Data only accessible to the Computer Security Team & Service Managers

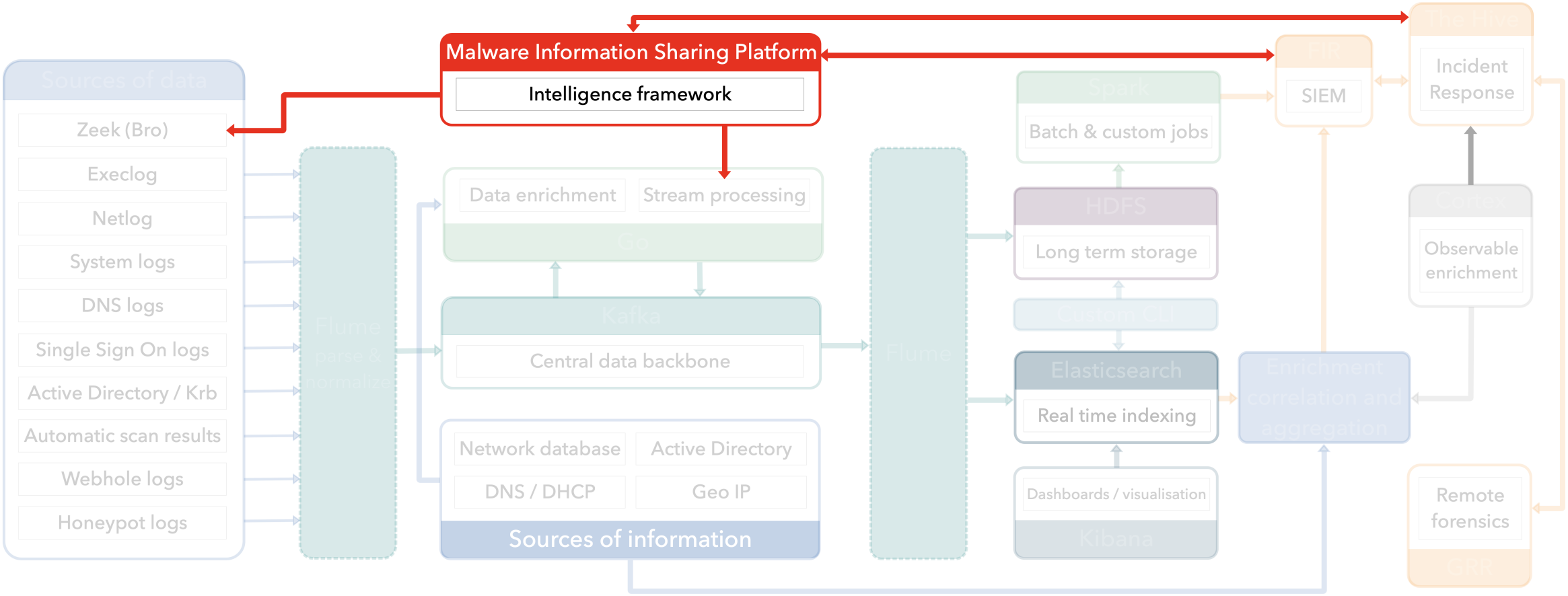
SYSTEM ARCHITECTURE



TECHNOLOGY STACK USED

- **Telemetry Capture Layer:** Apache Flume
- **Data Bus (Transport):** Apache Kafka
- **Analytics:** Apache Spark / Go
- **Long-Term Data Store:** Hadoop HDFS
- **Real-Time Index & Search:** Elasticsearch
- **Visualisation:** Kibana & CLI
- **Intrusion Detection:** Zeek (Bro)
- **Web frontends:** OpenShift

THREAT INTELLIGENCE



THREAT INTELLIGENCE

- MISP (Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing) as the sole threat intelligence platform at CERN
- Free and open source software for information sharing of threat intelligence including Indicators of Compromise (IoCs)
- Sharing is key to fast and effective detection of attacks

THREAT INTELLIGENCE

- CERN is currently operating 5 different instances:
  - Main CERN instance (~2.2 M IoCs)
  - Worldwide LHC Computing Grid (WLCG) central MISP instance (~1.2 M IoCs)
  - Development MISP instance used for MISP development (CERN is an active contributor) and for validating new MISP releases
  - Two community specific MISP instances

- We are currently actively sharing threat intelligence with ~540 peer organisations

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-ni-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

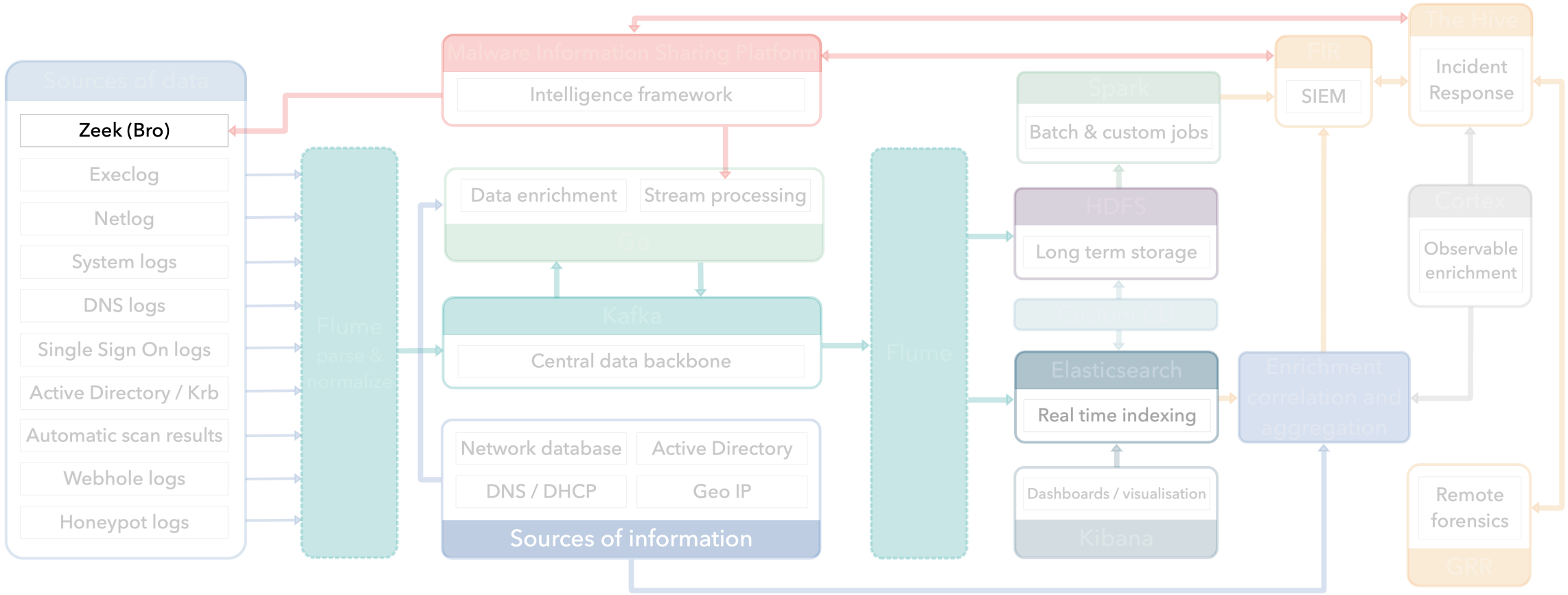
Event ID	8887
Uuid	5a9d1aa2-16c4-4100-8d44-0037ac130003
Source Organisation	
Member Organisation	CERN
Contributors	
Email	cert-ioc@cern.ch
Tags	tlp:white x circl:incident-classification="malware" x malware_classification:malware-category="Trojan" x circl:incident-classification="system-compromise" x +
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++XnUYmkMDiu8KuJXnFDJMkyXxsq77fOpDhVGOoexll3+P6SmZWVlWwnhOgvxhccgT72J+LPZElwPqPZQVHR4ksdVSnMVreyZs+rQ7O+L2xychpqzelrk4Q/08f5XreOnq4Rgxp9oKwSlf7vKmQ7tUWUxfMHHL1wQYZPmdKpgSi/JmokLpp5cKAT7r0gGOj1jV8ZAJc+z45Ts2JBH9JYscHBssh7MBWWymcjXANd9a6XaQnbnl6nOFFNyYm8dBuLkGpEUNCdMq/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

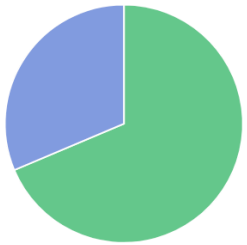


ZEEK INTRUSION DETECTION SYSTEM (IDS)

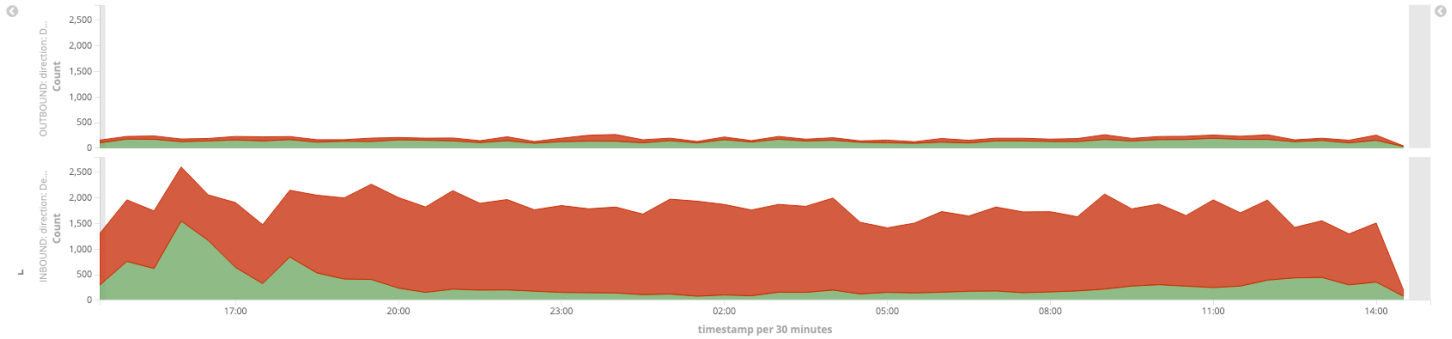
- Comprehensive logging of activity for offline analysis and forensics
- Port-independent analysis of application-layer protocols
- Out of the box support for many application-layer protocols including: DNS, FTP, HTTP, IRC, SMTP, SSH, SSL
- Analysis of file content, including MD5 / SHA1
- Real-time integration of external Indicators of Compromise
- Support for IDS-style pattern matching
- Event-based programming model

ZEEK: SSH TRAFFIC

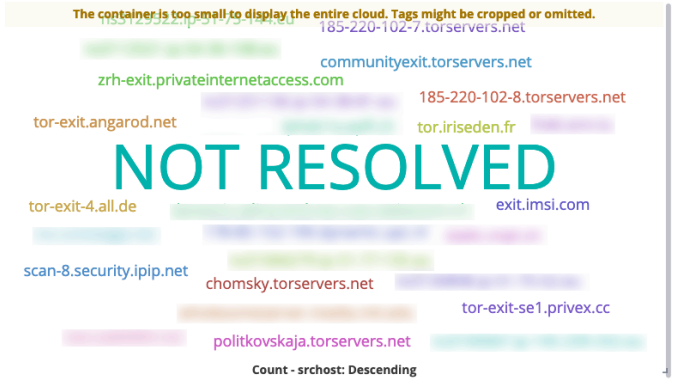
Zeek: SSH Successful connections



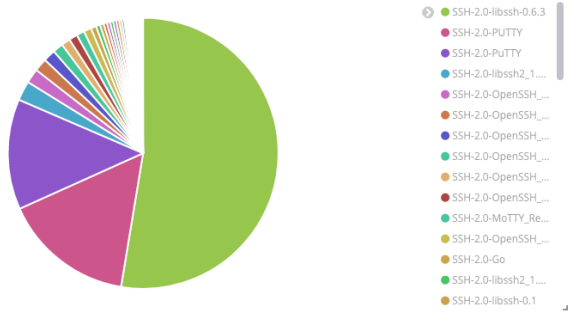
Zeek: SSH Authentication over time



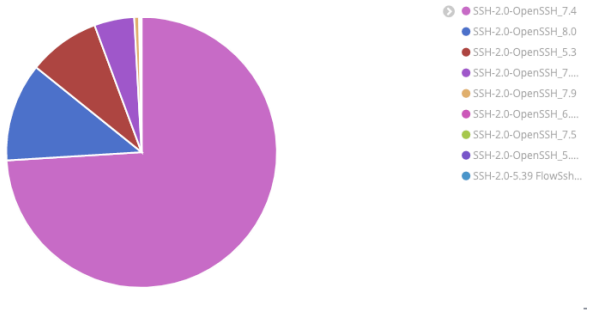
Zeek: SSH 50 external hosts with the most failures



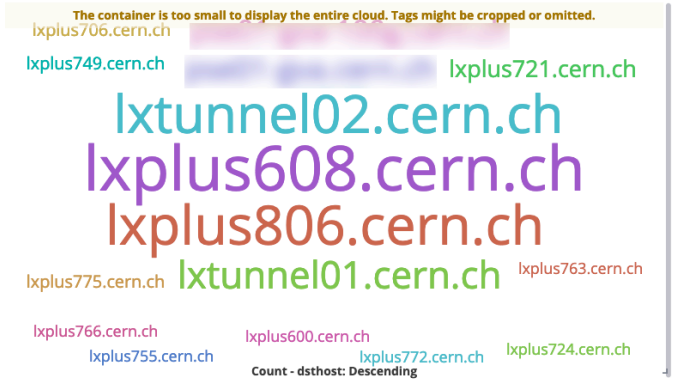
Zeek: SSH External Client versions



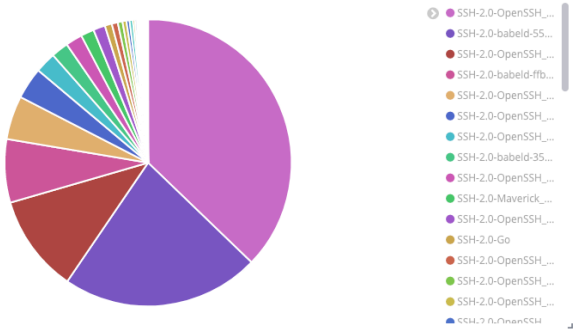
Zeek: SSH CERN Server versions



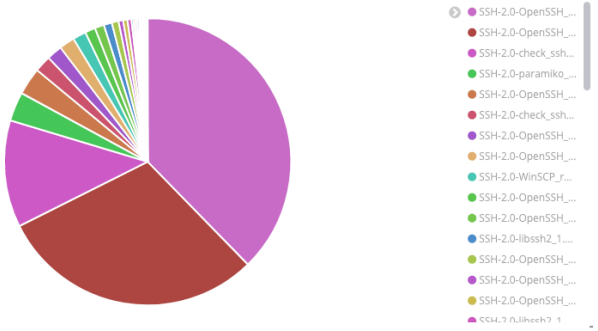
Zeek: SSH 50 most active servers (hostnames)



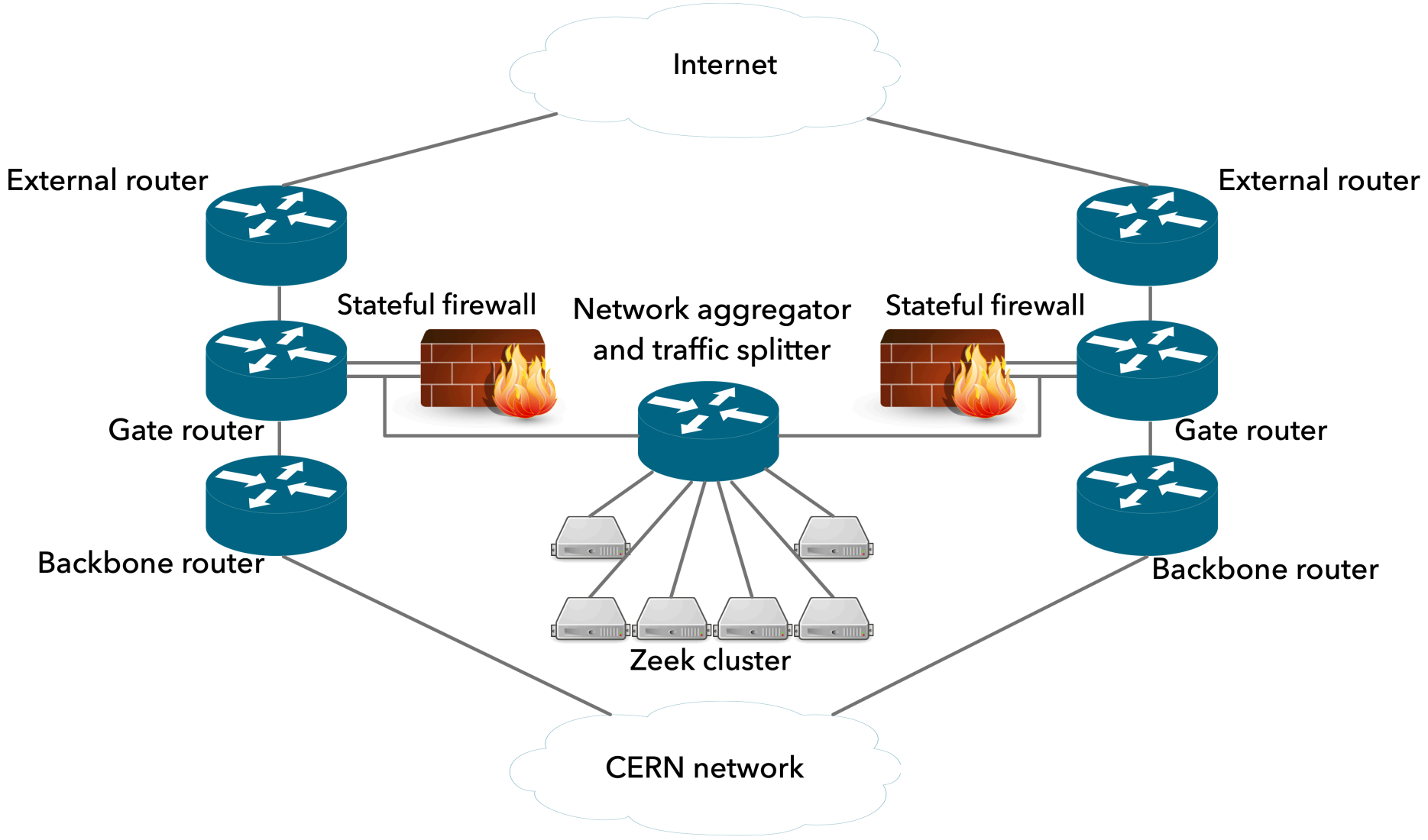
Zeek: SSH External Server versions



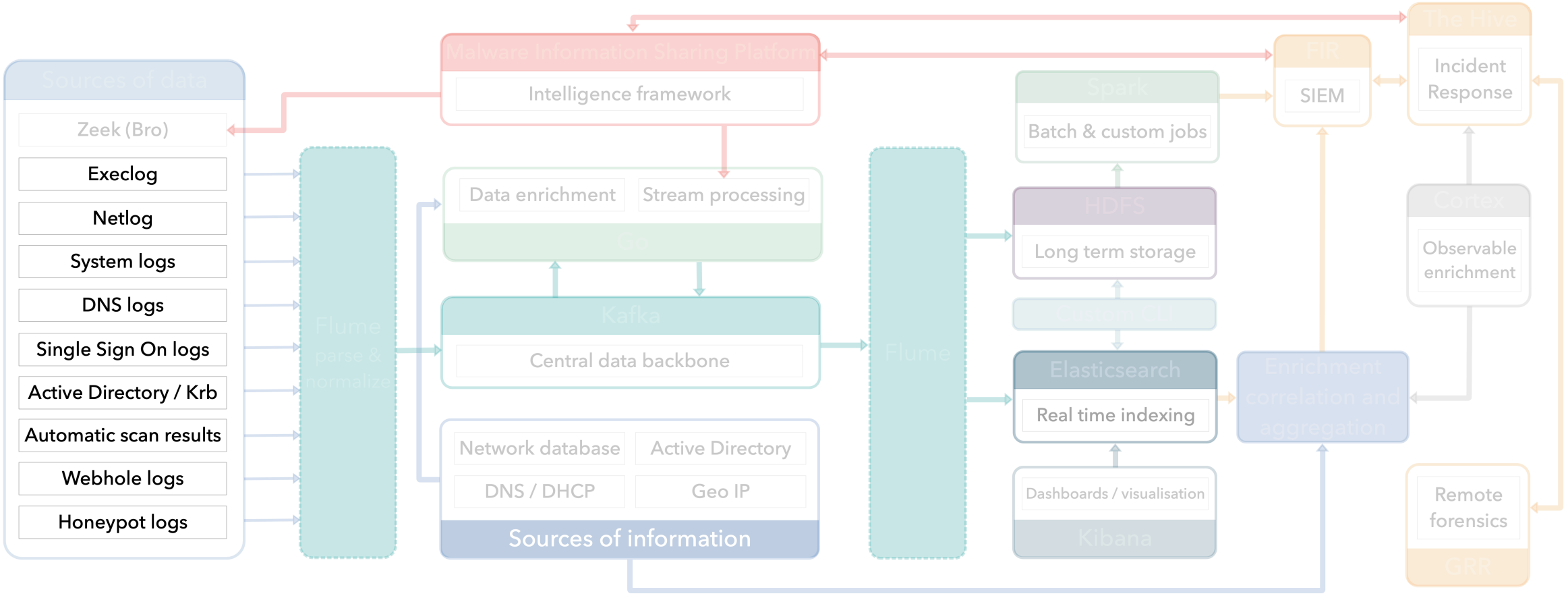
Zeek: SSH CERN Client versions



NETWORK TRAFFIC AGGREGATOR AND SPLITTER



OTHER SOURCES OF DATA

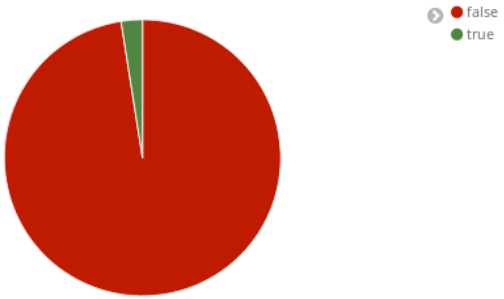


SYSTEM LOGS, EXECLOG, NETLOG

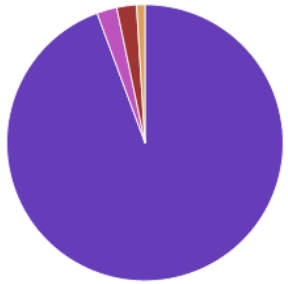
- Standard system logs
  - Collected in collaboration with IT monitoring: same Flume agent
  - sshd log extraction: login / logout, Kerberos principal used
  - Collected from interactive and batch clusters

- Extended activity logs: Execlog and Netlog
  - Same collection mechanism (shared Flume)
  - For shared systems, traceability down to the user & process
    - Deployed on interactive clusters
  - Produced by custom kernel modules (kprobes)
    - Project to re-implement via auditd / go-audit

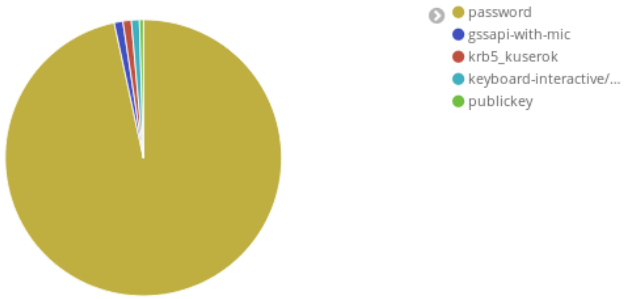
CSL: SSH success



CSL: SSH Type

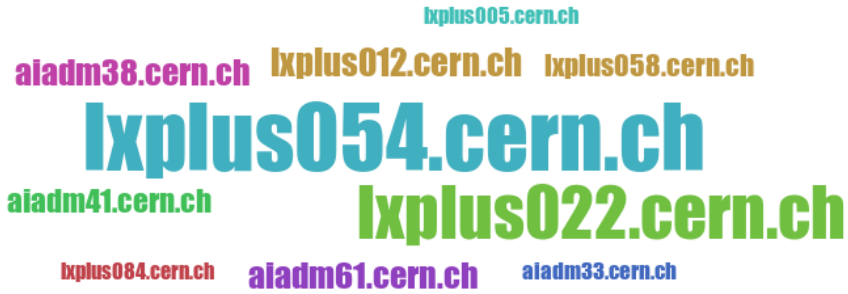


CSL: SSH Method



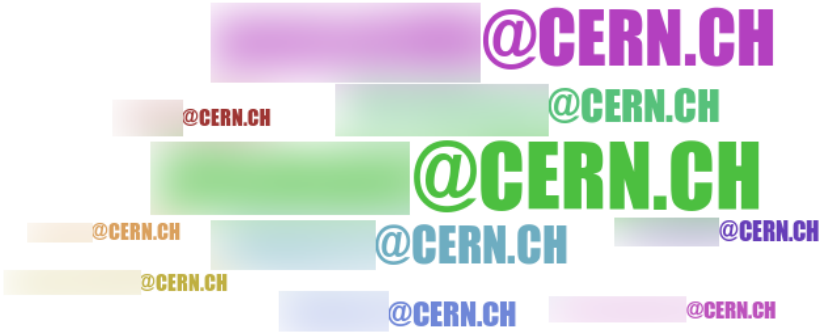
CSL: SSH srcip

CSL: SSH Host



CSL: SSH user

CSL: SSH Principal



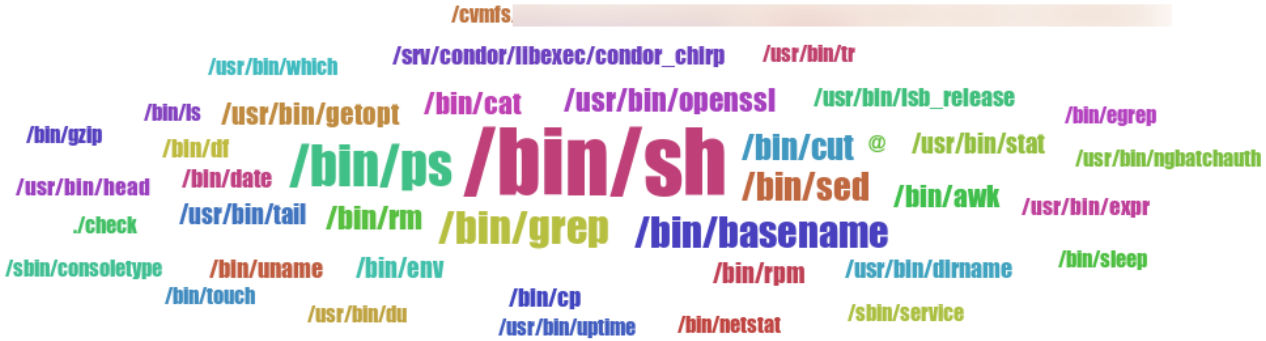
CSL: Execlog SID

CSL: Execlog UID

CSL: Execlog EUID

CSL: Execlog Host

CSL: Execlog File



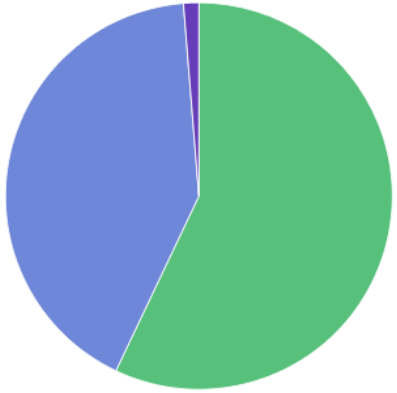
WEBHOLE

- 3 types of sink-holing in place:
  - Typo-squatting / mistyped domains
  - SWITCH DNS Firewall
  - Blocked by CERN Security Team (phishing, malware, …)

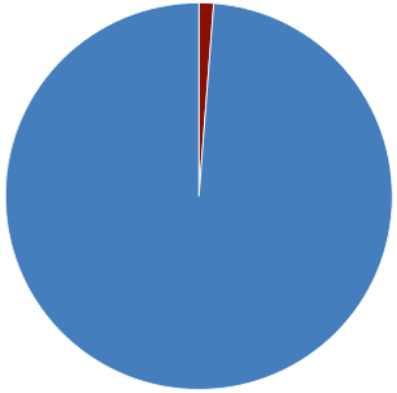
- Logs collected:
  - From Apache redirection logs: srcip, domain & referrer (full)
  - Parsed and forwarded using Flume

CSL: Webhole Domain

CSL: Webhole Hostgroup



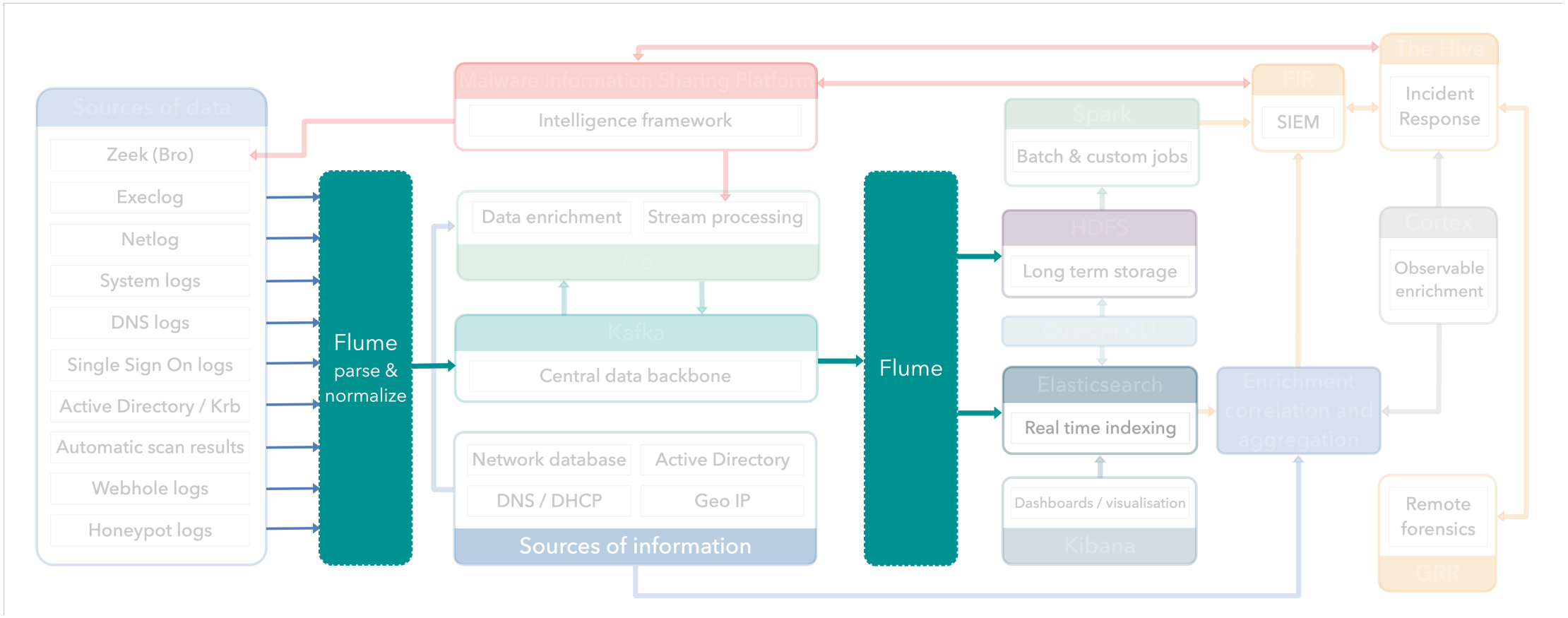
CSL: Webhole Source (CERN or external)



CSL: Webhole Referrer

The container is too small to display the entire cloud. Tags might be cropped or omitted.

FLUME TRANSPORT

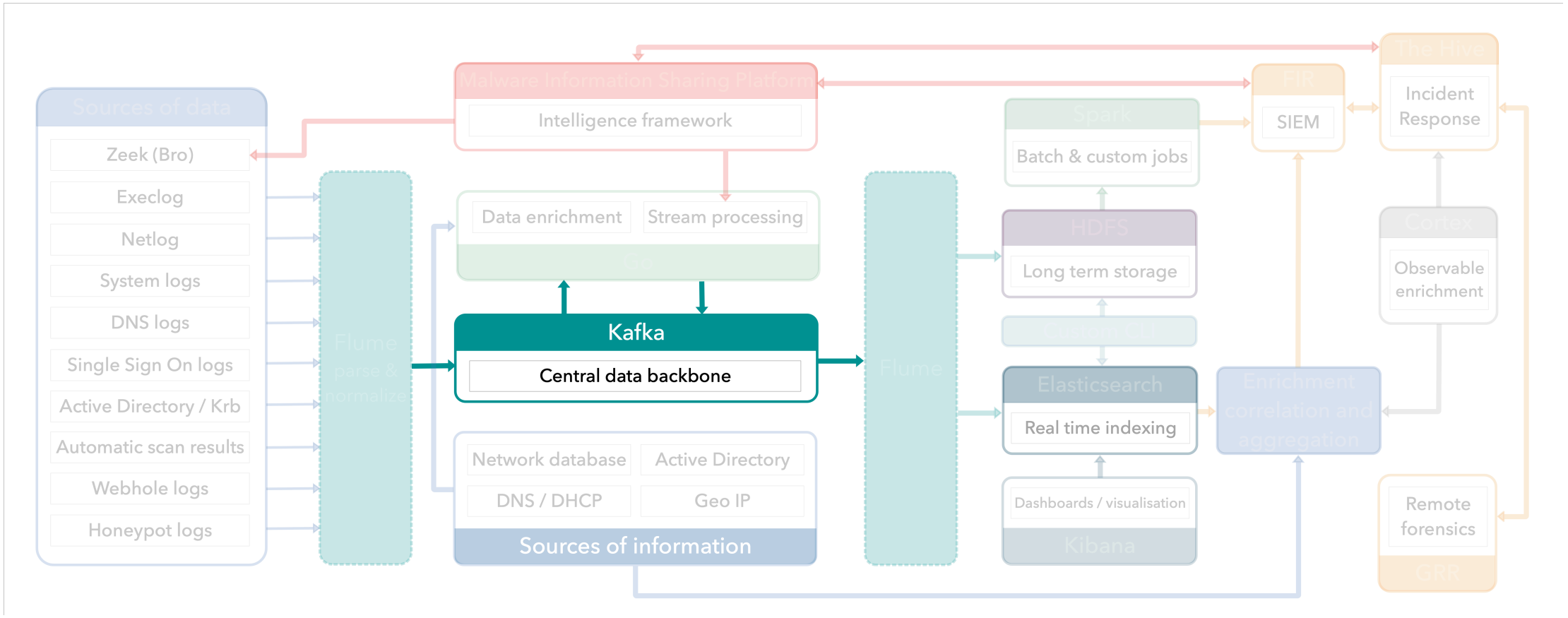


FLUME TRANSPORT

- Similar to IT monitoring infrastructure
  - Same base packages and design
  - Custom interceptors, Elasticseach sink patches
  - Data ingress, log parsing and normalisation
- "Pre" Kafka:
  - Receive data from agent deployed by IT monitoring + ours
  - Validate, parse, normalise, pre-process data
- "Post" Kafka:
  - Push data to Elasticsearch & HDFS
  - Optimisations to support high throughput to Elasticsearch

MONITORING OF FLUME GATEWAYS

KAFKA DATA BACKBONE



KAFKA DATA BACKBONE

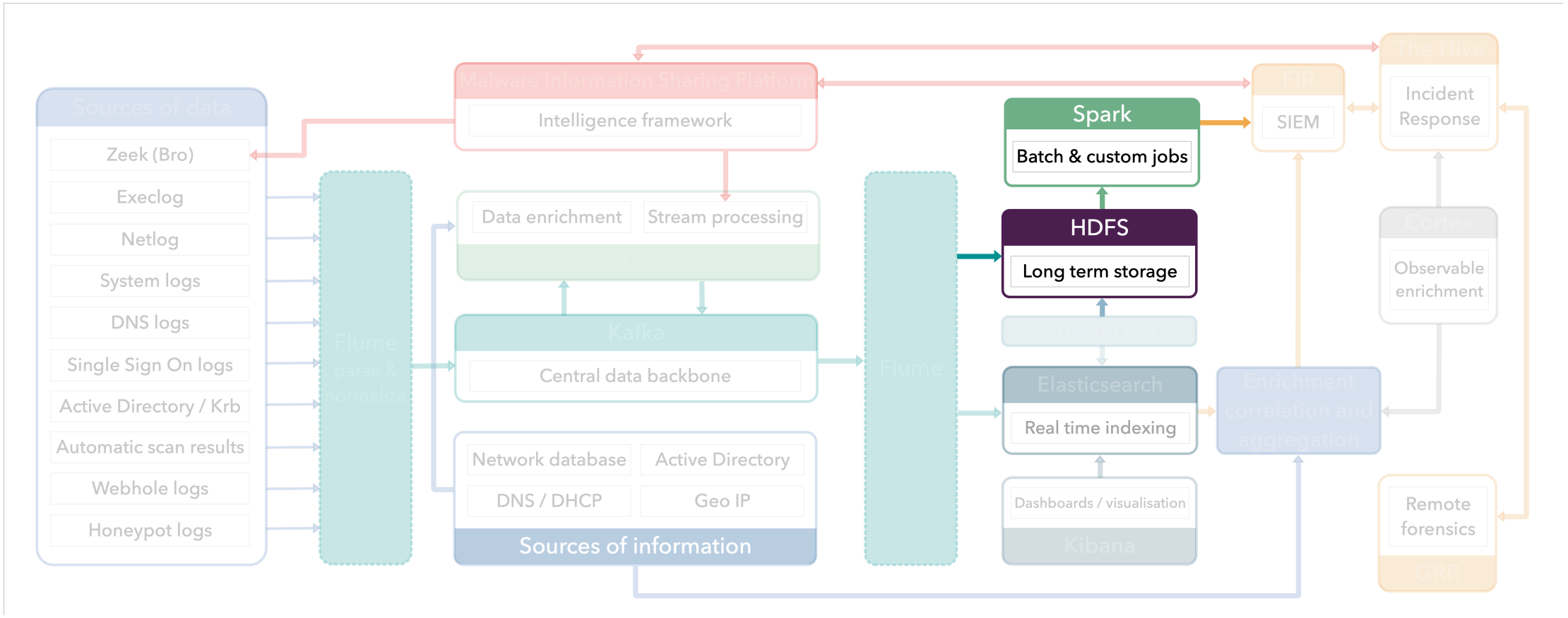
- Using the central Kafka service
  - First users of the central Kafka service
  - Helped test & validate cluster setup and security features

- 6 Kafka brokers, 3 Zookeeper nodes
  - ~100,000 messages / sec on average
  - 72 hours retention period
  - Replication factor of 3
  - Data compressed using zlib

KAFKA DATA BACKBONE

- 83 topics (209 partitions)
  - 1 topic with 18 partitions
  - 5 topics with 12 partitions each
  - 10 topics with 6 partitions each
  - 2 topics with 3 partitions each
  - 65 topics with 1 partition each

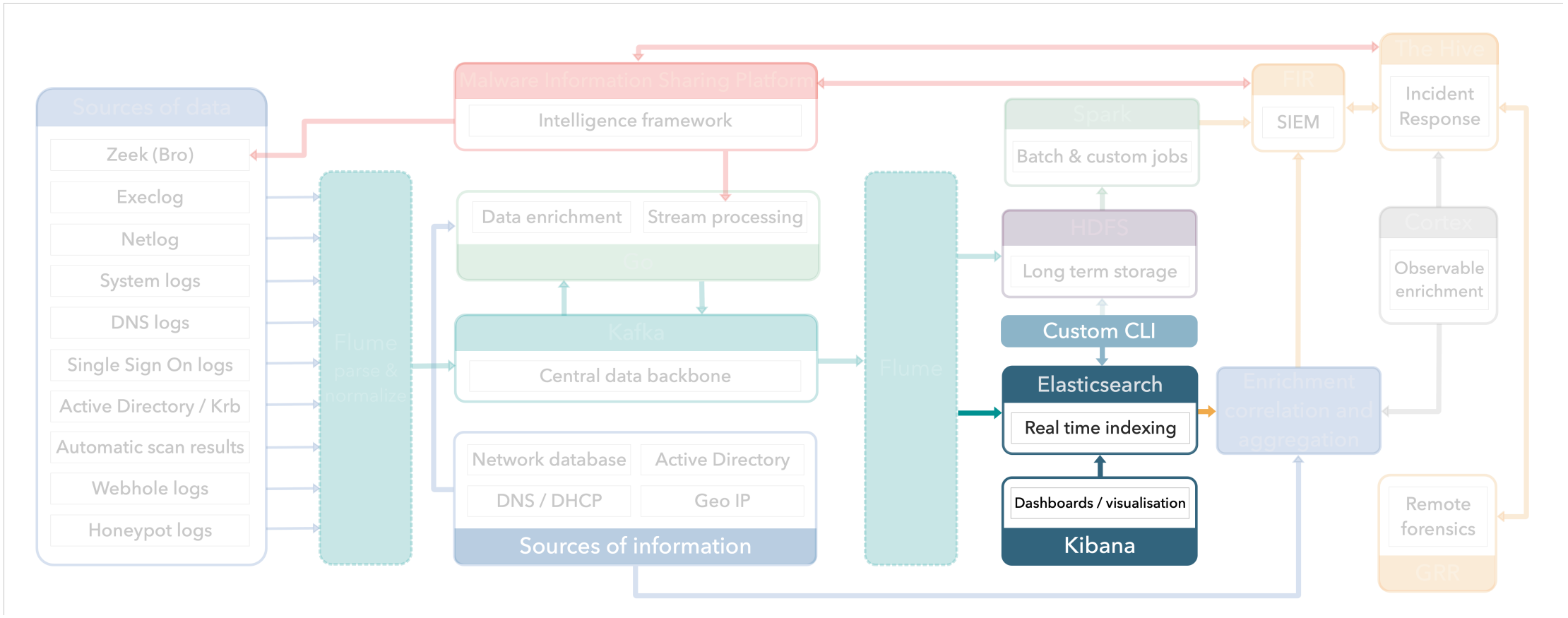
HDFS STORAGE



HDFS STORAGE & DATA ACCESS

- Long term storage: 13 months (400 days)
- Staged:
  - Raw JSON logs written by Flume
  - [Ongoing] Daily conversion to Parquet using Apache Spark
    - 8x compression ratio
- Raw data rates for 6st of July 2020 (x 3 due to replication):
  - Zeek: 2.5 TiB / day
  - Other log sources: 0.6 TiB / day
- Current use: analysis using Spark
  - Working on adding batch jobs for advanced correlation and aggregation.

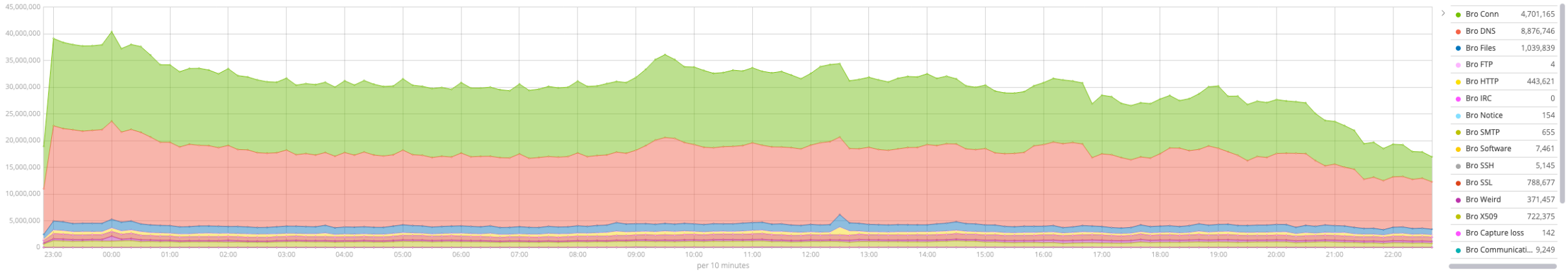
ELASTICSEARCH STORAGE



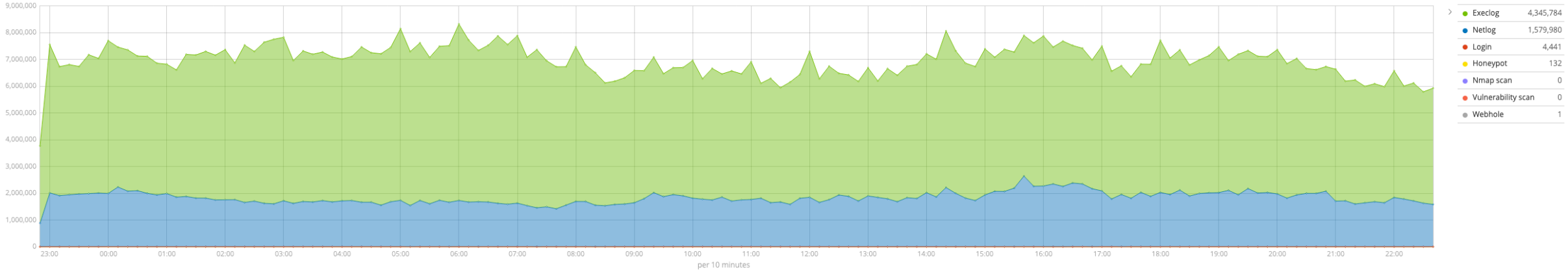
ELASTICSEARCH STORAGE & DATA ACCESS

- Short term storage: 90 days
- Two different dedicated clusters from the central Elasticsearch service:
  - One cluster for Zeek data
  - Another cluster for all other sources of data
- Data rates for 6th of July 2020 (x 2 due to replication):
  - Zeek: 4.9 billion documents, 1.46 TiB
  - All other sources of data: 1.1 billion documents, 0.25 TiB
- Current use:
  - Real time access and visualisation
    - Kibana and custom CLI

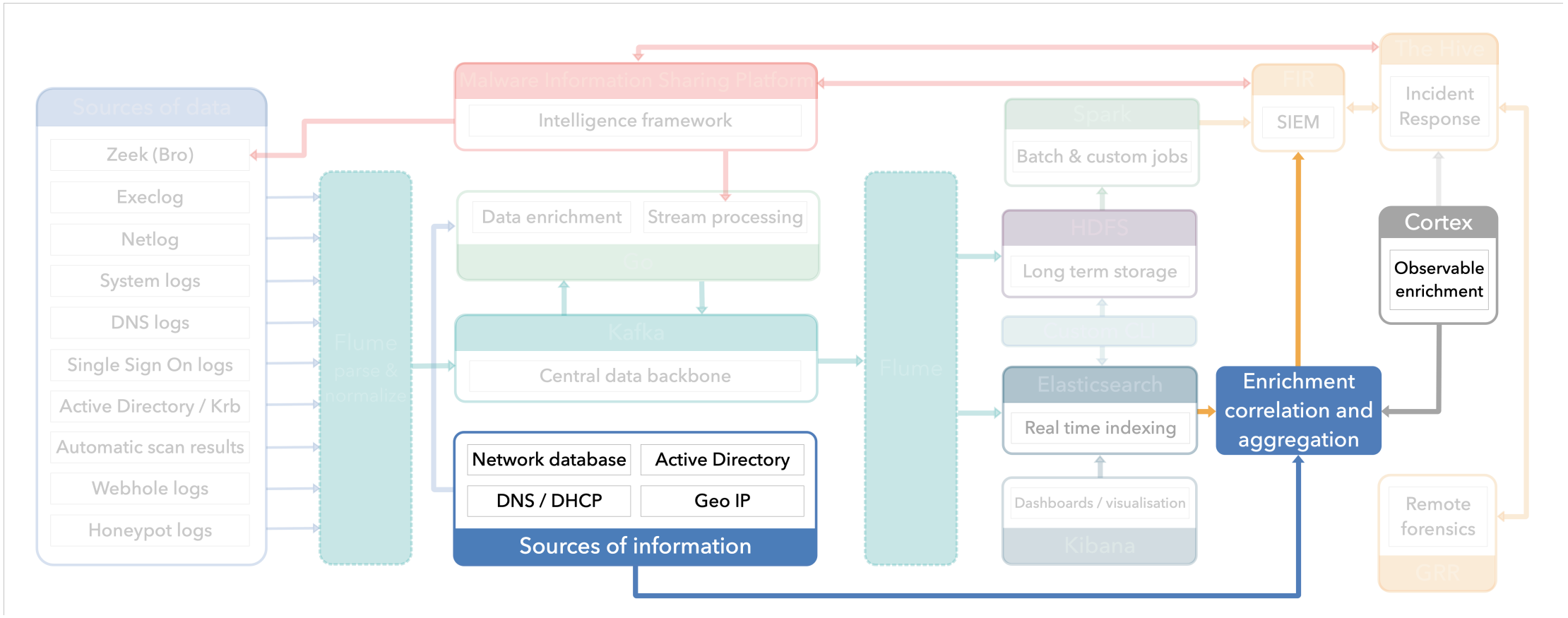
ELASTICSEARCH - LOGS BY TYPE



CSL: logs by type



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

CERN Document Server Alert Engine <noreply@cern.ch>
[CERT SOC] [redacted] 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	[redacted]	212.83.133.112 No IDS 212.129.56.50 No IDS	42	2018-02-22	[redacted]	tlp:white osint:source-type="blog-post"

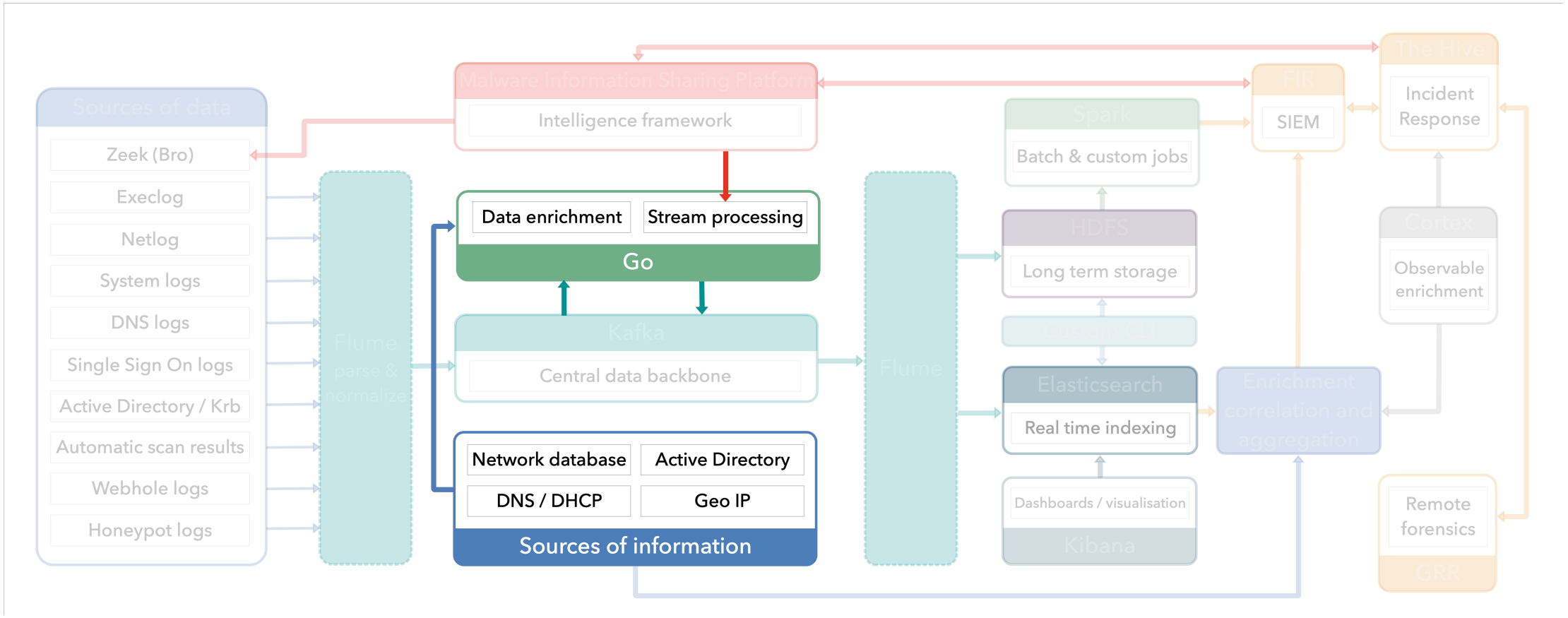
Basic connection details

Time	IoC triggering alert	Source	Destination	Application	Other actions
2018-03-07 12:36:41	212.83.133.112	[redacted]	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	[redacted]	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	[redacted]	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	[redacted]	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=1520422600215673607211373814534140 1&SUB_ID=1436235&v_id=lQiFXVpkoa_KFKK5842Qvkql44TPU34qbordrCquBpc.		200	OK

GO STREAMING PROCESSING



INLINE PROCESSING

- Previously using Apache Spark structured streaming
- Custom code written in golang
  - Jobs launched and monitored using Nomad
  - Running distributed on Nomad clients Data ingested from Kafka
- Types of jobs:
  - Data enrichment:
    - DNS (forward and reverse DNS resolutions)
    - GeoIP
  - Intrusion detection:
    - Based on IoCs from MISP
    - Custom, advanced rules
  - Monitoring
  - More to come

DATA ENRICHMENT

- Very fast, not guaranteed to be 100% accurate

- DNS resolution
  - Golang routines: highly asynchronous
  - ~1-3 sec delay for entries that can not be resolved
  - Filtering what messages to enrich

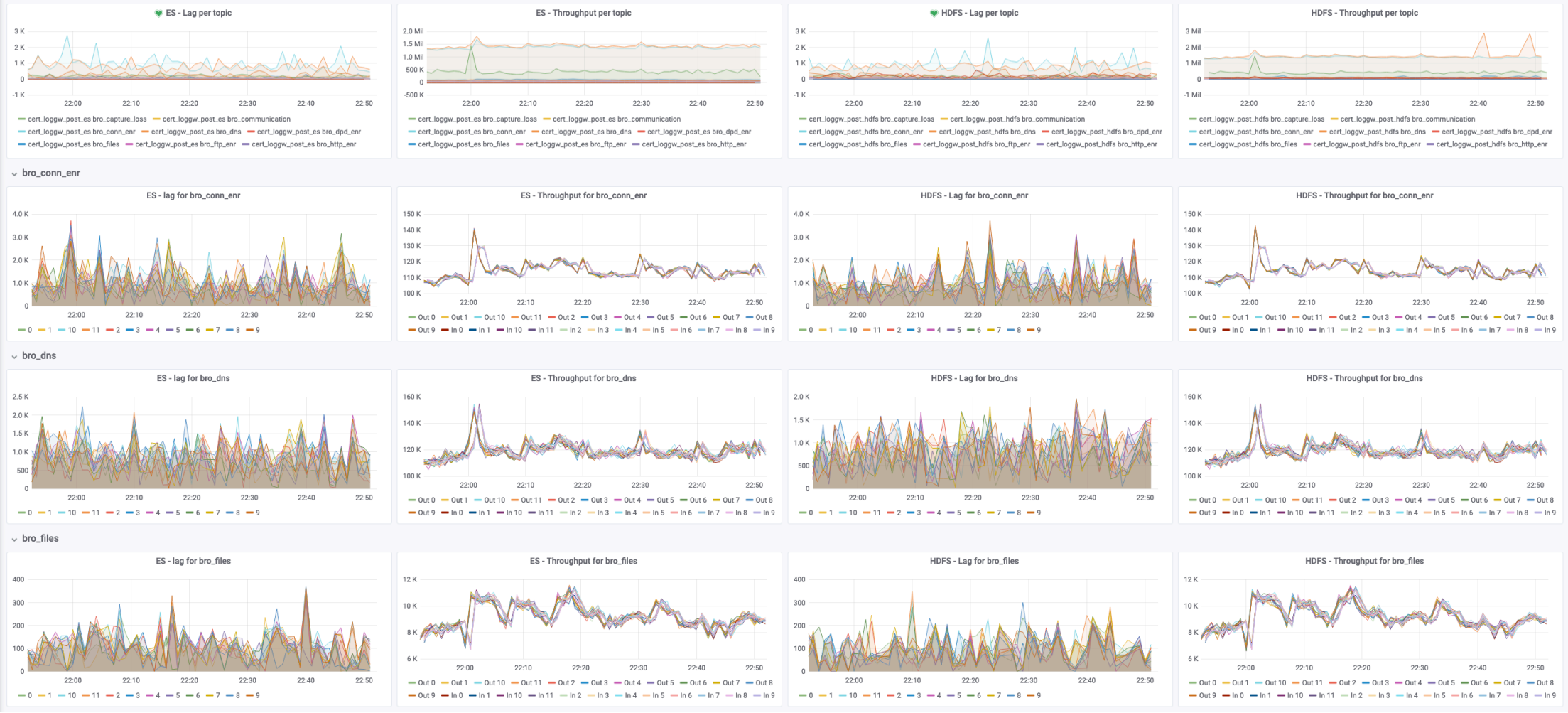
MONITORING

- Collectd plugins:
  - Custom developed plugins
    - Check last timestamp and volume of data in source and destination Kafka topics
    - Consumer groups and Kafka topics
    - Using Python Kafka libraries based on librdkafka

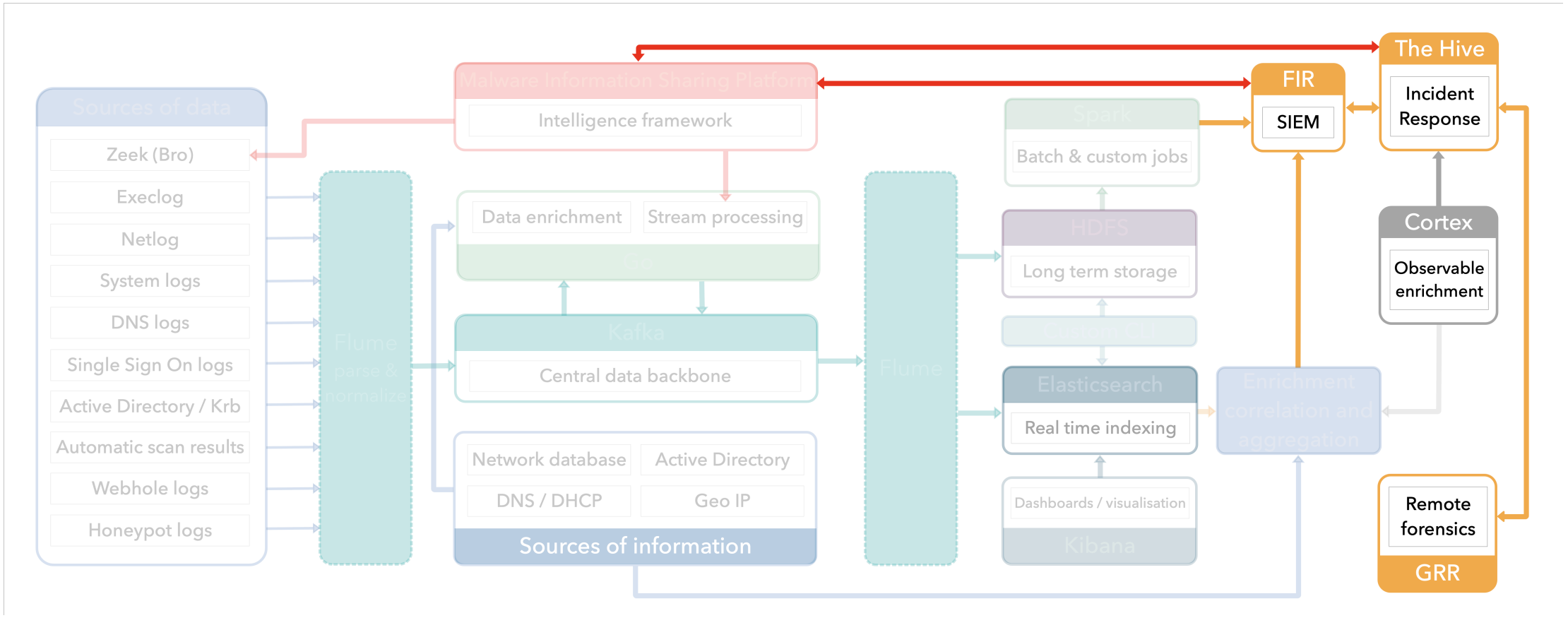
- Ad hoc scripts to produce monitoring of the monitoring data (i.e. inject dummy data)

TOPIC MONITORING (LAG & ENRICHMENT)

CONSUMER GROUP (FLUME) MONITORING



INCIDENT MANAGEMENT & RESPONSE



INCIDENT MANAGEMENT & RESPONSE

- 4 open-source tools employed:
  - FIR (Fast Incident Response): SIEM (Security Incident Event Management) tool for the common user-facing incidents
  - The Hive: used for complex / sensitive incidents, more powerful analysis than FIR
  - Cortex: provides observable (Indicator of Compromise) analysis capabilities
  - GRR Rapid Response: remote forensics

FIR: FAST INCIDENT RESPONSE

- Developed by CERT Société Générale: https://github.com/certsocietegenerale/FIR
- Easy creation and tracking of security incidents for the team
- Internal CERN fork → user interaction module, REST API extensions and SSO
  - CERN improvements & extensions pushed upstream
- Incidents created by SOC, CLI or manually
- Written in Django
- CI deployment on Openshift

FIR DASHBOARD (I)

- Main security team dashboard

FIR | New event | Dashboard | Incidents | Events | Stats | search... | Currently logged in as **admin** [logout] [Admin]

STARRED INCIDENTS

No incidents to show.

Open | Blocked | Old | Tasks

Date		Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Edit
2018-03-07	☆	Accounts/Copyright violation	Copyright infringement detected on [CRISTI-PC]	ischuszt	2	Open	CERT	None	User Answered 3 hours ago	None	C0	admin	
2018-03-07	☆	Accounts/Compromised	Compromised account for ischuszt	ischuszt	1	Open	SOC	None	Opened 3 hours ago	None	C0	admin	
2018-03-07	☆	Devices/Compromised	Hello world	ischuszt	1	Open	SOC	None	Opened 3 hours ago	None	C0	admin	
2018-03-05	☆	Accounts/Compromised	Account compromised - ischuszt	ischuszt	1	Open	SOC	None	Opened 2 days ago	None	C0	admin	
2018-03-05	☆	Devices/Compromised	Device compromised: cristi-pc	ischuszt	1	Open	SOC	None	Opened 2 days ago	None	C0	admin	

FIR DASHBOARD (II)

- Incident details

FIR | New event | Dashboard | Incidents | Events | Stats | search... | Currently logged in as **dev** [logout] [Admin]

Incident Leader None | **Plan** None | **Severity** 1 | **Category** Phishing | **Status** Closed | **Detection** CERT | **B/L** Demo BusinessLine 1

Incident / Phishing / test

Opened on Jan. 15, 2015, 5:47 p.m. by dev

DESCRIPTION

phishing copying our brand website on http://evilwebsite.com/evilurl

detected by one of our clients

TO-DO LIST

Action	Accountable
Contact registrar	CERT

+ Add To-Do Item

CORRELATED ARTIFACTS

Type	Values
Hostnames	evilwebsite.com (2)

RELATED FILES

Date	File	Description
Feb. 5, 2015, 5:20 p.m.	MongoHub.zip	
Feb. 5, 2015, 5:50 p.m.	YARA_User_s_Manual_1.6__1_.pdf	yara

Browse... | Upload files | Download archive

ATTRIBUTES

Name	Value
loss	2784

+ Add attribute

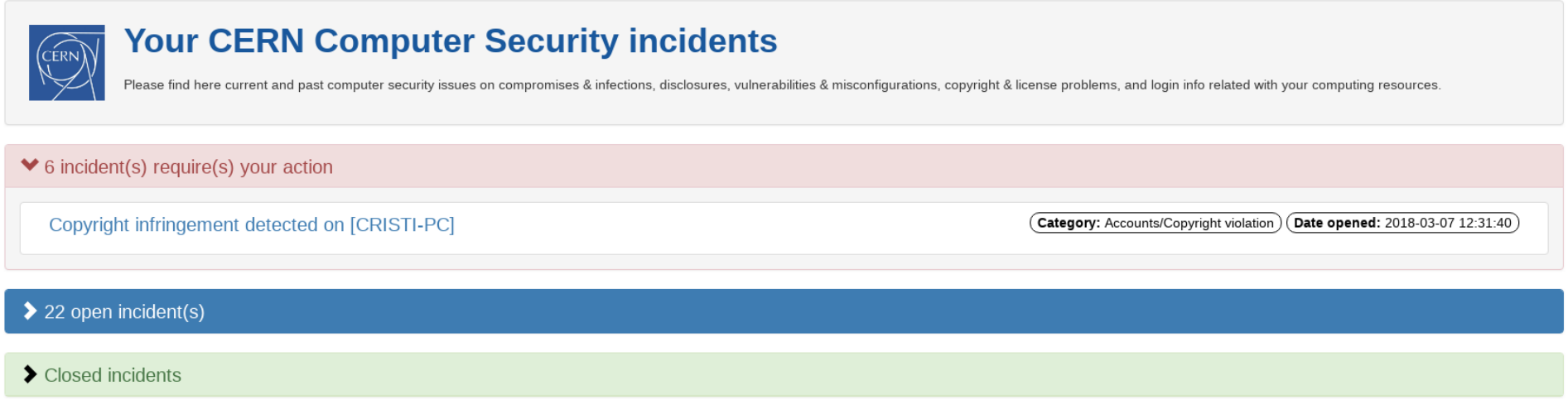
Comments (3) | Artifacts (2)

		Comment	Action
2015-02-09 14:32	dev	new test	Monitor
2015-01-30 19:10	dev	Changed "status" from "Closed" to "Open"; Changed "is_starred" from "True" to "False";	Info
2015-01-15 17:47	dev	Incident opened	Opened

Add | Comment | Edit | Open | Block | Incident followup | Alert | Takedown

FIR USER INTERACTION (I)

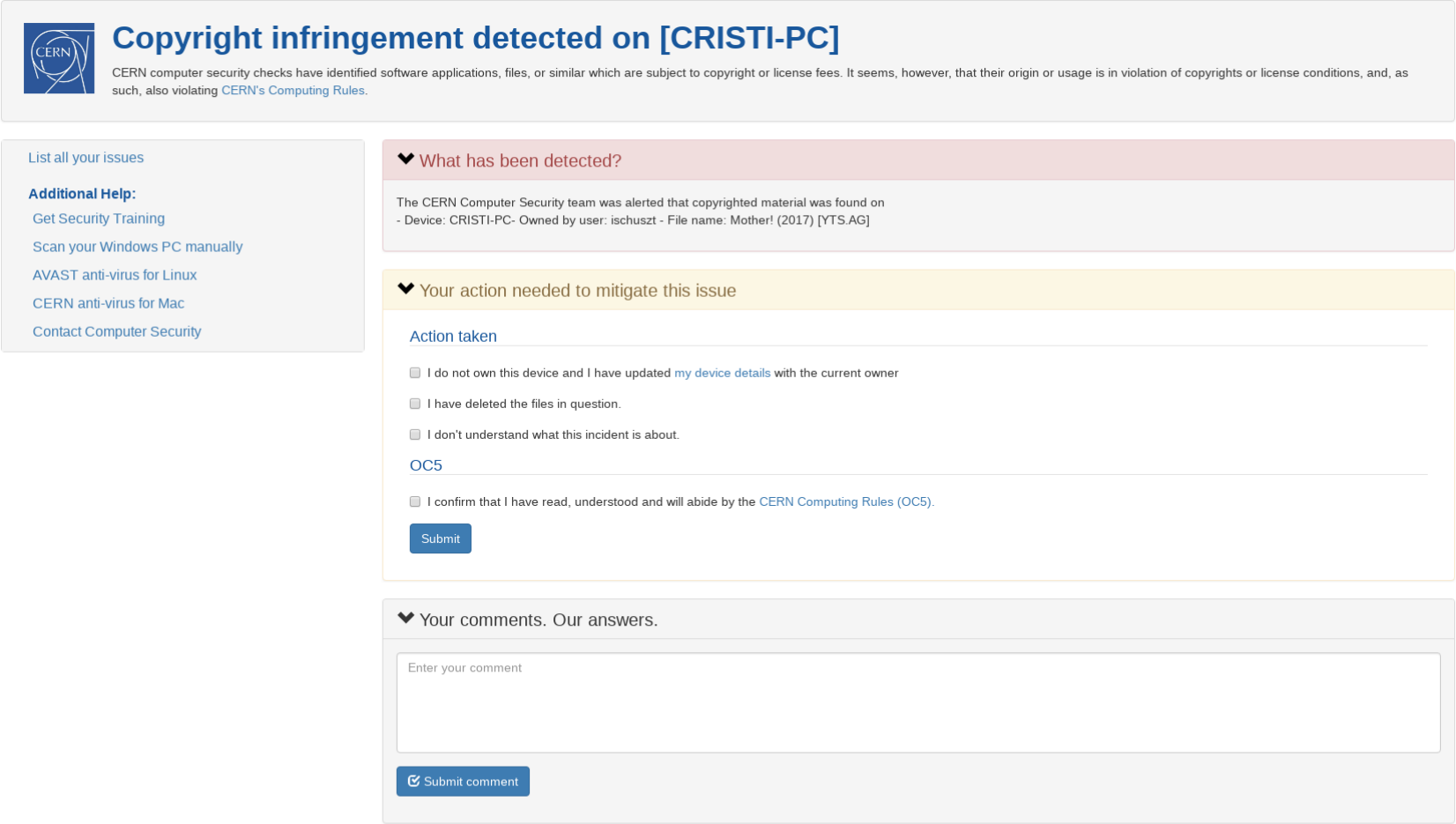
- Unified hub for every user's security incidents and a way of communicating with the security team (email is not ideal)
- ACLs: restricted views only to incidents impacting the user



FIR USER INTERACTION (II)

- Dynamic mitigation form generated according to incident

- State change notifications and comments



SECURITY ALERTS UI: BEFORE AND AFTER

Security Alert on your Device

Use this portal to mitigate your event yourself!

Event Details

Device: **LERYA-BIS**

Owner: **VINCENT BRILLAULT**

Status: **BLOCKED**

Additional Help

- Scan your Windows PC manually
- CERN anti-virus for Windows (for free!)
- CERN anti-virus for Mac
- AVAST anti-virus for Linux
- Kaspersky TDSSKiller
- MSRT
- Update the owner of this device
- Disconnect this device
- Contact Computer Security
- Get Security Training

About...

- CERN Computing Rules (OC5)
- How to secure your PC
- Virus
- Malware
- Rootkit detection

What has been detected?

CERN computer security checks have detected malicious activity on your device. This is a strong indication that your device has been infected, broken into and compromized.

Activity details:

TEETST□□□T

Your action to mitigate this problem:

Please check this device for signs of a break-in, identify the application(s) ca activity and take actions to prevent this in future.

- ☐ I have disabled/removed the application causing this alert.
- ☐ I have run a full antivirus scan with the latest virus signature files and/or a full scan with Kaspersky TDSSKiller, or MSRT.
- ☐ I have checked for unexpected files or running processes.
- ☐ I have formatted the device and reinstalled its operating system.
- ☐ I have updated the owner of this device, since I do not own it anymore.
- ☐ I have disconnected this device, as I do not need it anymore.
- ☐ [I have done something else]

These basic steps might not always work, the cause might be triggered by something different, or this alert might be a false alarm. Thus, in case of problems, please indicate the issues you are facing to resolve this problem:

- ☐ Neither the antivirus software nor the antimalware tool found anything suspicious.
- ☐ I do not know what caused the problem: [Further details]

If you have questions or need help, please contact Computer.Security@cern.ch.

Further points you should check:

This potentially malicious activity might have already impacted on your digital assets. Even if you reinstall your device, the attackers might still have access to them...

Copyright infringement detected on [CRISTI-PC]

CERN computer security checks have identified software applications, files, or similar which are subject to copyright or license fees. It seems, however, that their origin or usage is in violation of copyrights or license conditions, and, as such, also violating CERN's Computing Rules.

- List all your issues

Additional Help:

- Get Security Training
- Scan your Windows PC manually
- AVAST anti-virus for Linux
- CERN anti-virus for Mac
- Contact Computer Security

What has been detected?

The CERN Computer Security team was alerted that copyrighted material was found on
- Device: CRISTI-PC- Owned by user: ischuszt - File name: Mother! (2017) [YTS.AG]

Your action needed to mitigate this issue

Action taken

- ☐ I do not own this device and I have updated my device details with the current owner
- ☐ I have deleted the files in question.
- ☐ I don't understand what this incident is about.

OC5

- ☐ I confirm that I have read, understood and will abide by the CERN Computing Rules (OC5).

Submit

Your comments. Our answers.

Enter your comment

Submit comment

THE HIVE

- Advanced open source incident response platform: https://github.com/TheHive-Project/TheHive
- Integration with MISP events, powerful search capability

TheHive | + New Case | My tasks 0 | Waiting tasks 2 | Alerts 1012 | Dashboards | Case, user, URL, hash, IP, domain ... | Admin | CS Cristian Schuszter

List of alerts (1012 of 4687)

No event selected | Quick Filters | Sort by | Stats | Filters | 15 per page

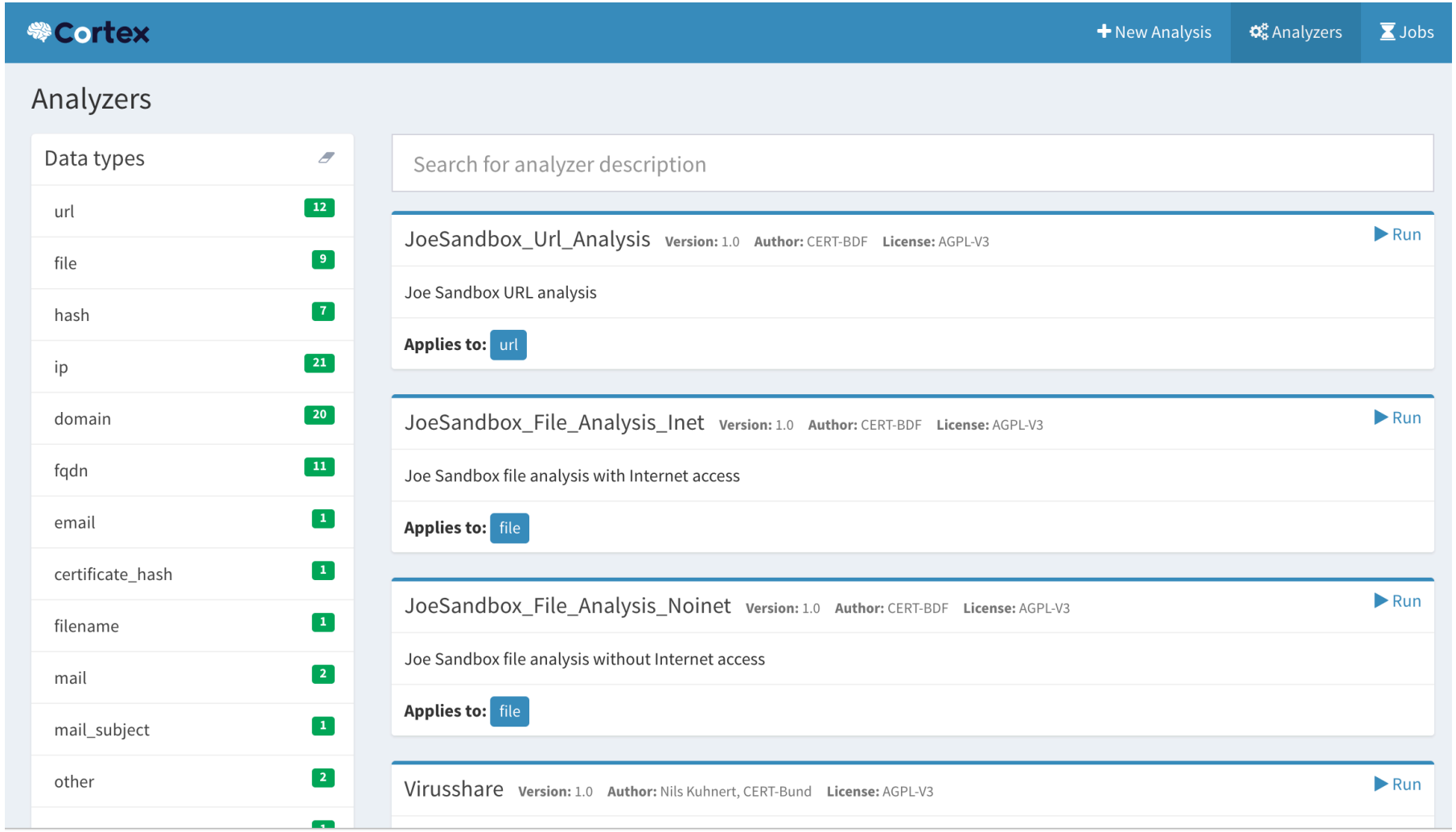
1 filter(s) applied: **Status:** New, Updated ✖ Clear filters

First | Previous | 1 | 2 | 3 | 4 | 5 | ... | Next | Last

Reference	Type	Status	Title	Source	Severity	Attributes	Date
8907	misp	New	#8907 "faktura - T-mobile" src:CERT PKO BP, MalSpam, vjw0rm	misp-dev	L	17	Wed, Mar 7th, 2018 15:57 +01:00
8906	misp	New	#8906 Cobalt Gang Activity (2018-03-07) src:ZKB, APT, misp-galaxy:threat-actor="Cobalt"	misp-dev	M	23	Wed, Mar 7th, 2018 14:18 +01:00
8904	misp	New	#8904 "F-ra VAT" Campaign src:CERT PKO BP, Banker, MalSpam, Nymaim	misp-dev	L	18	Wed, Mar 7th, 2018 14:07 +01:00
8903	misp	New	#8903 M2M - Malspam delivers W32/VBInject + Pony src:GTO-CERT, malware:Pony	misp-dev	L	21	Wed, Mar 7th, 2018 12:34 +01:00

CORTEX

- Powerful and extendable analyzers for observables, The Hive & MISP integration: https://github.com/TheHive-Project/Cortex



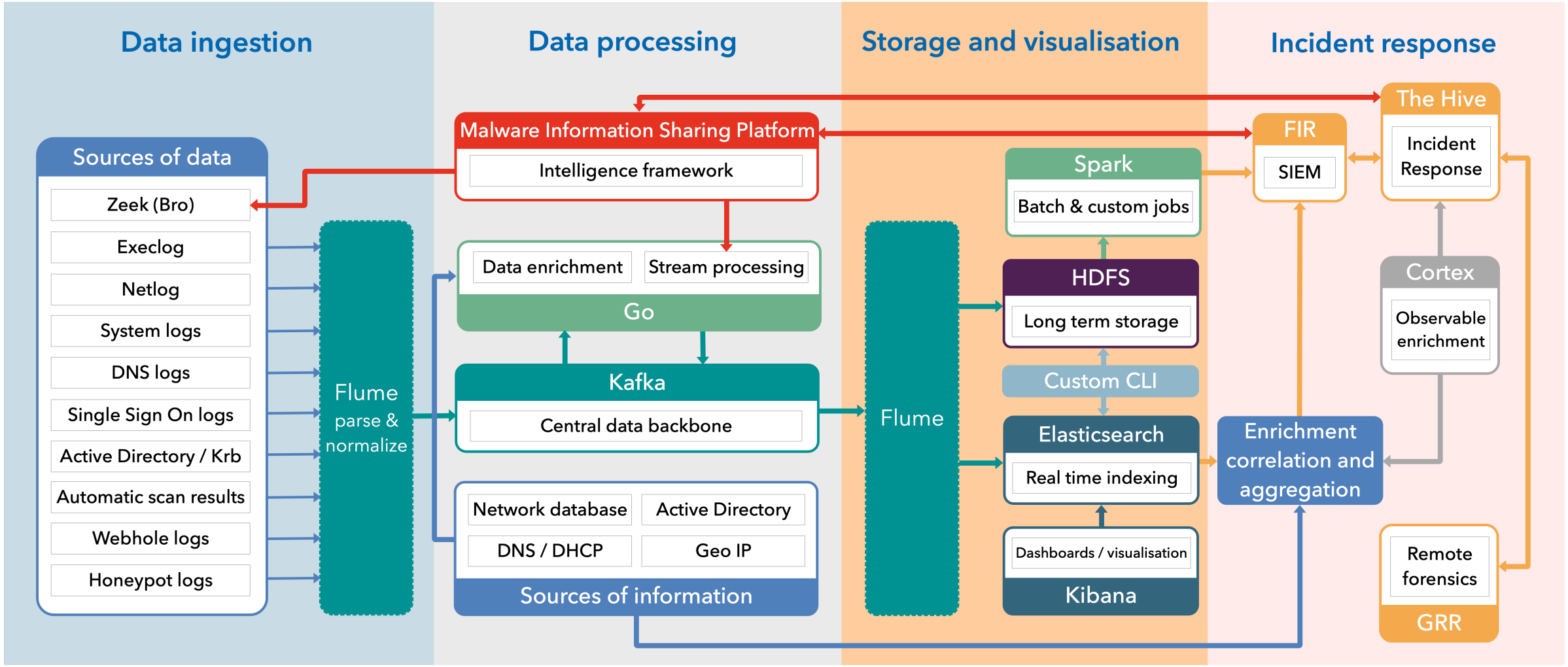
GRR RAPID RESPONSE

- Agent based remote forensics investigation tool
- Developed by Google: https://github.com/google/grr
- Features:
  - System information (hardware, users, ...)
  - Advanced remote forensics (files, registry, process list, ...)
  - Raw disk access
  - Process memory acquisition / scanning
  - and many more...

GRR RAPID RESPONSE

- Clients for Windows, Mac, Linux
  - Stable, robust, low-impact
  - Python + PyInstaller
  - Memory, CPU limited
  - Watchdog process
- Packaged but not installed
  - Installation only in case of an incident and with user consent
- Strong audit controls in place
  - Advanced, detailed audit logs
  - Approval-based system built in
    - User, reason, expiry

SYSTEM ARCHITECTURE



SHARING OF KNOW HOW

- CERN SOC as a reference for HEP, academia and others
  - WLCG SOC working group
    - Helping WLCG sites to deploy SOC capabilities
  - SWITCH Central Logging for Security
    - Service being implemented for Swiss universities
  - Collaboration inside trusted vetted circles with peers from industry and governmental organisations.

- Hands on technical workshops given at CERN

CONTRIBUTING BACK TO THE COMMUNITY

- CERN SOC based entirely on open source solutions
- Contributing upstream improvements and bug fixes
- MISP:
  - SSO authentication
  - Native export into Zook intel framework
  - Puppet module
- Zeek:
  - RPM packaging, fixes and improvements to build process
  - Extensions to intel framework
- FIR:
  - User interaction module
  - API extensions
- The Hive:
  - SSO authentication

CERN