THREAT INTELLIGENCE
FOR THE ACADEMIC COMMUNITY

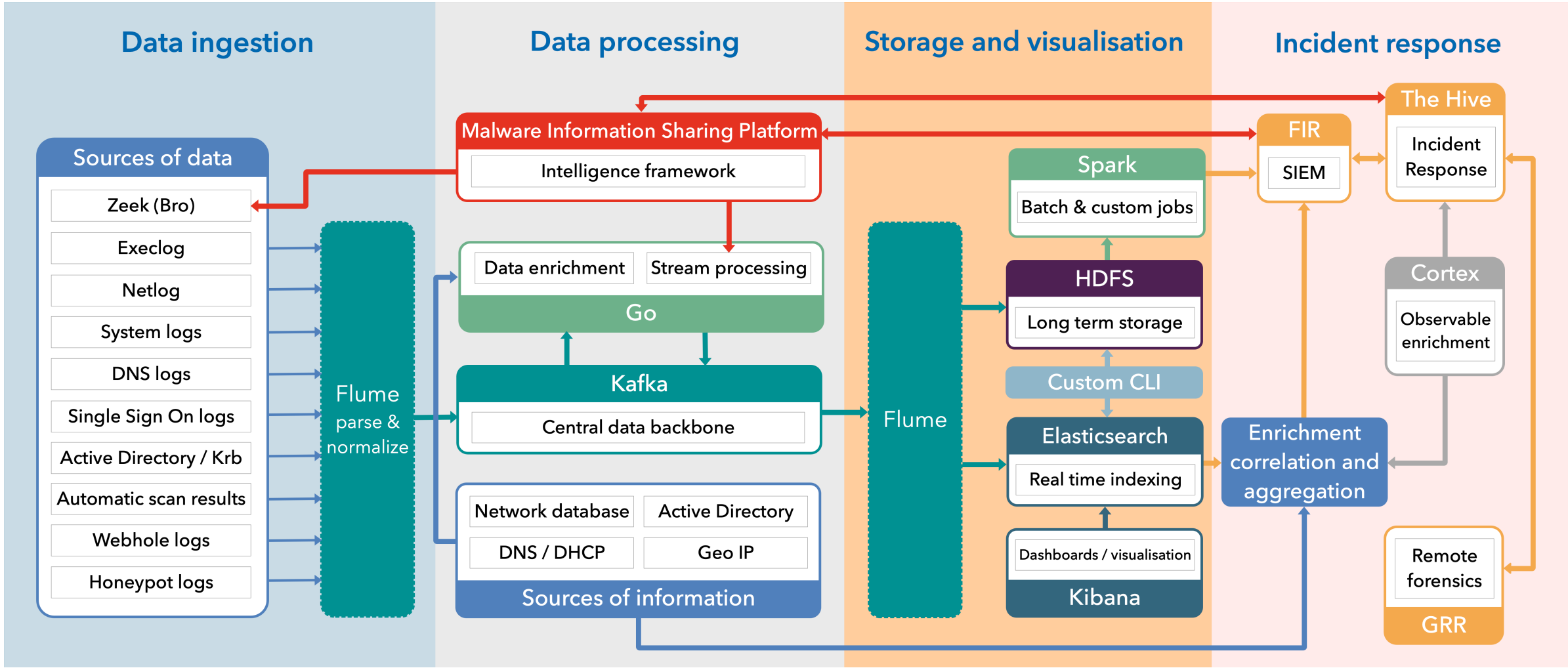
LIVIU VÂLSAN

17TH OF AUGUST 2020

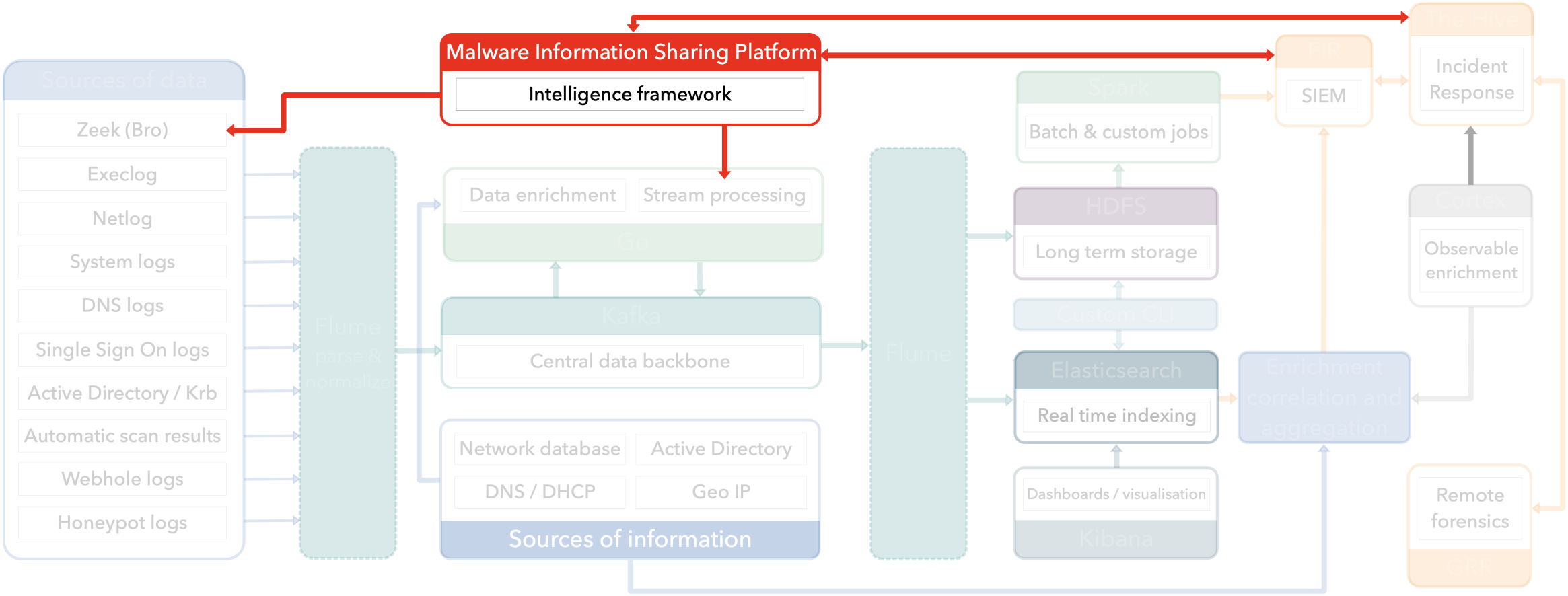
SYSTEM DESIGN OF THE CERN SOC

- 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

SYSTEM ARCHITECTURE OF THE CERN SOC



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 (~2.3 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 ~570 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-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++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)		

ACCESS TO THREAT INTELLIGENCE

- Access to the Academic MISP instance governed by a Threat Intelligence Sharing Agreement
  - Rules of engagement
  - Use of the threat intelligence shared using this instance
- Information usage policy
  - Threat intel exclusively for the benefit of the trusted parties
  - Solely for the purpose of detecting, containing, mitigating and resolving security attacks

ACCESS TO THREAT INTELLIGENCE

- Commitments
  - Follow and obey the TLP guidelines and sharing restrictions
  - Follow and obey the SCIv2 trust framework assertions IR1-4
  - Follow and obey the information usage policy
  - Share back information whenever you believe it may be beneficial to a trusted party and are in a position to do so

CONTACT DETAILS

- Website
  - wlcg-soc-wg.web.cern.ch
- Documentation
  - wlcg-soc-wg-doc.web.cern.ch
- Mailing list
  - wlcg-soc-wg@cern.ch
- David Crooks (david.crooks@cern.ch)
- Liviu Vâlsan (liviu.valsan@cern.ch)
- Access to Academic MISP instance:
  - wlcg-security-officer@cern.ch