Una piattaforma unificata di Observability, Compliance e Security

Alessandro Fortunati
CTO @ Seacom

#OSW2021

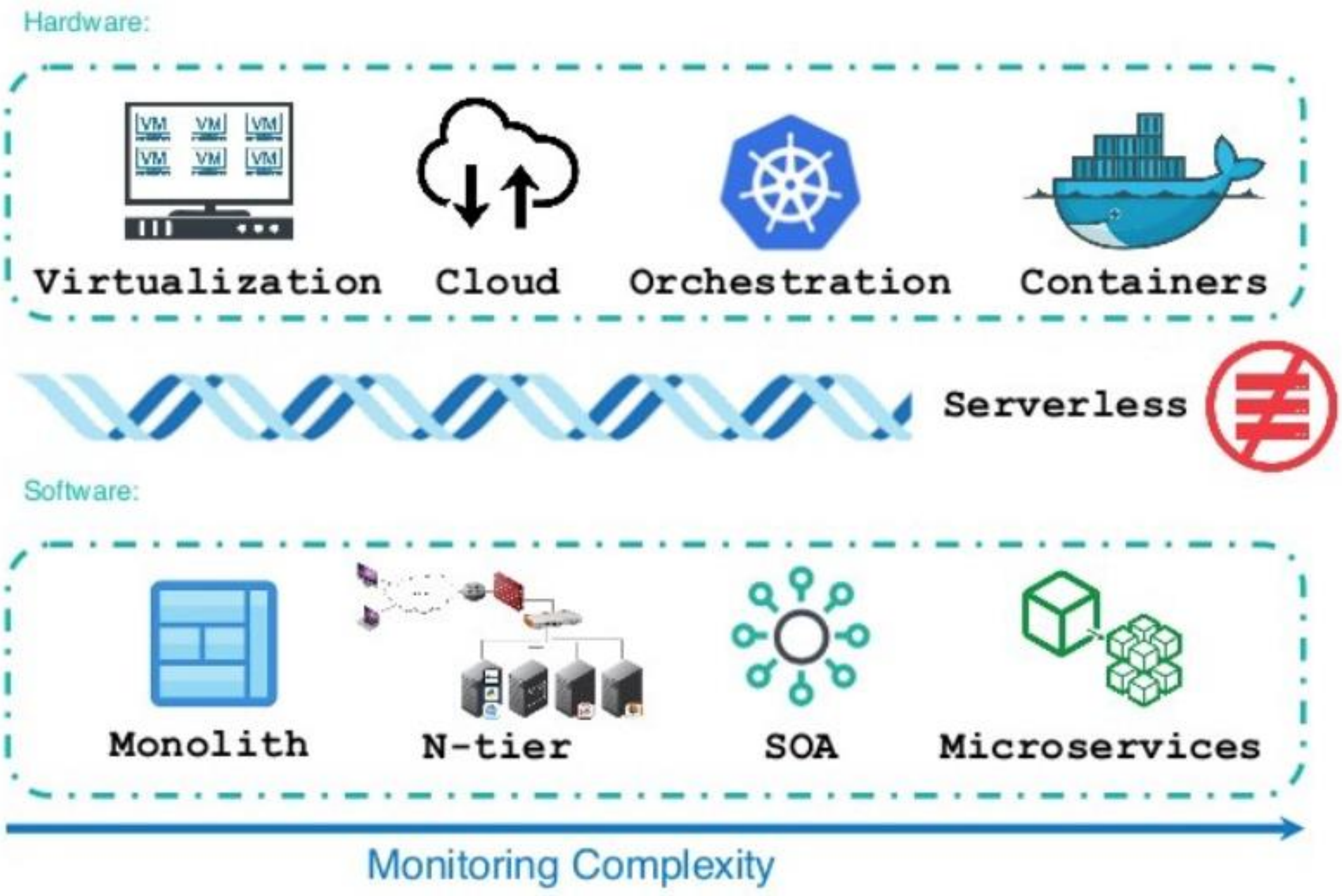
Observability

OSSERVABILITA’

Un sistema si dice osservabile se è possibile determinarne lo stato nel tempo

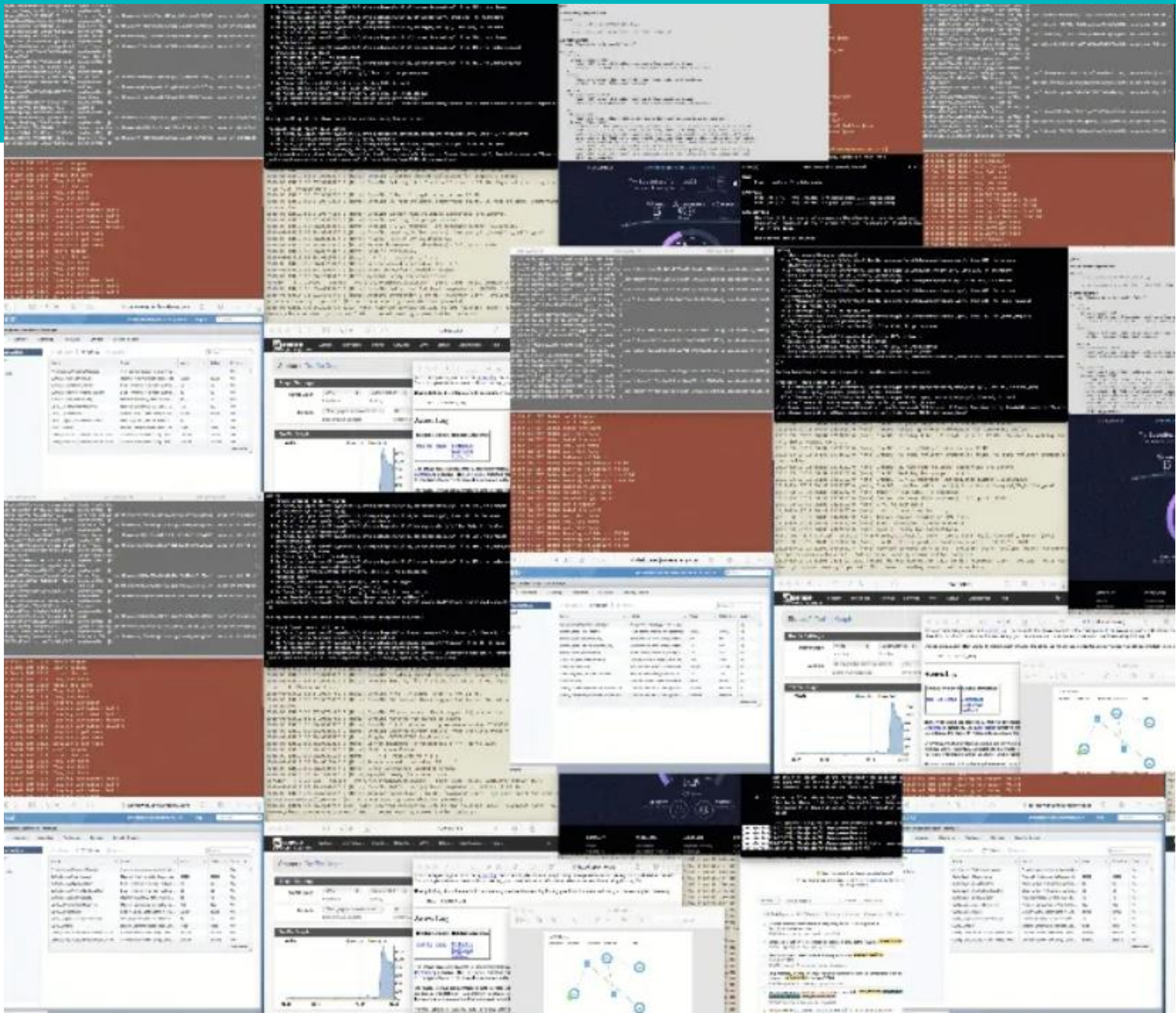
ARCHITETTURE IN EVOLUZIONE

A seguito della continua **evoluzione** delle architetture **HW** e **SW** implementare una soluzione di **monitoraggio** centralizzato risulta sempre più problematico



LA DISPERSIONE

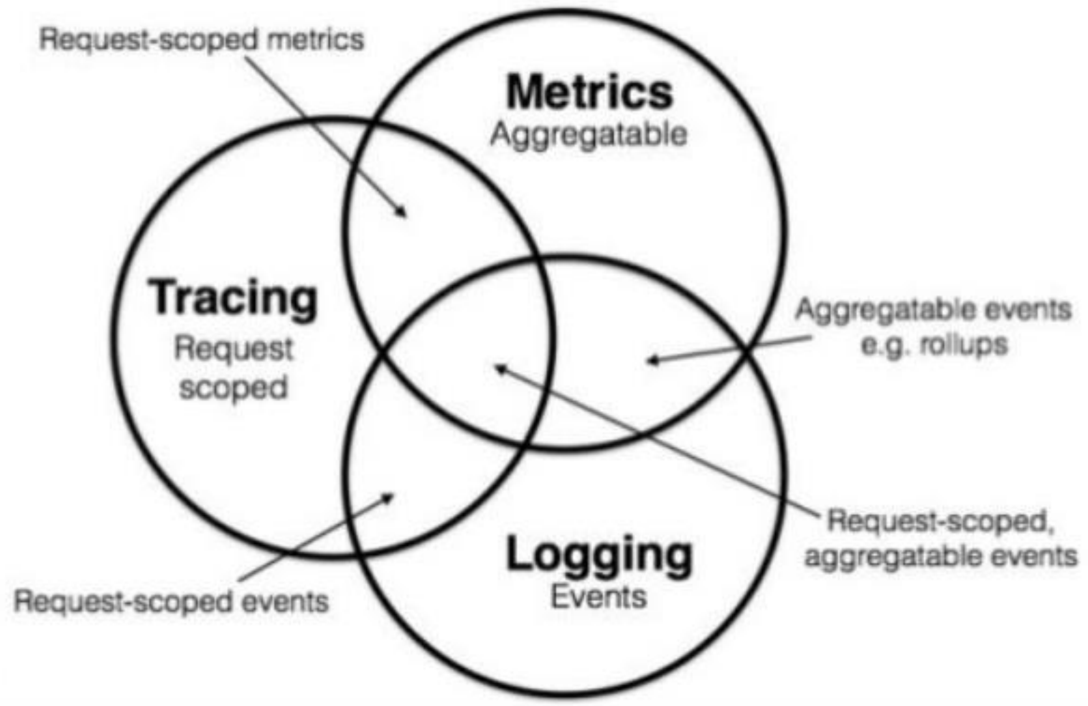
Il numero di **eventi** e la loro **eterogeneità** unite a svariate soluzioni di **monitoraggio** portano alla esigenza di concentrare in un unico punto di **osservazione**



OSW2021 OPENSOURCEWEEK

I PILASTRI

Log, Metric e Trace sono le fondamenta dell' observability il posizionamento della applicazione di monitoraggio determina la capacità di osservazione



SCHEMA COMUNE

La adozione di uno **schema** comune è la chiave per la **aggregazione** e **correlazione** degli **eventi** seppur **eterogenei**

Group 1 (Must be populated)

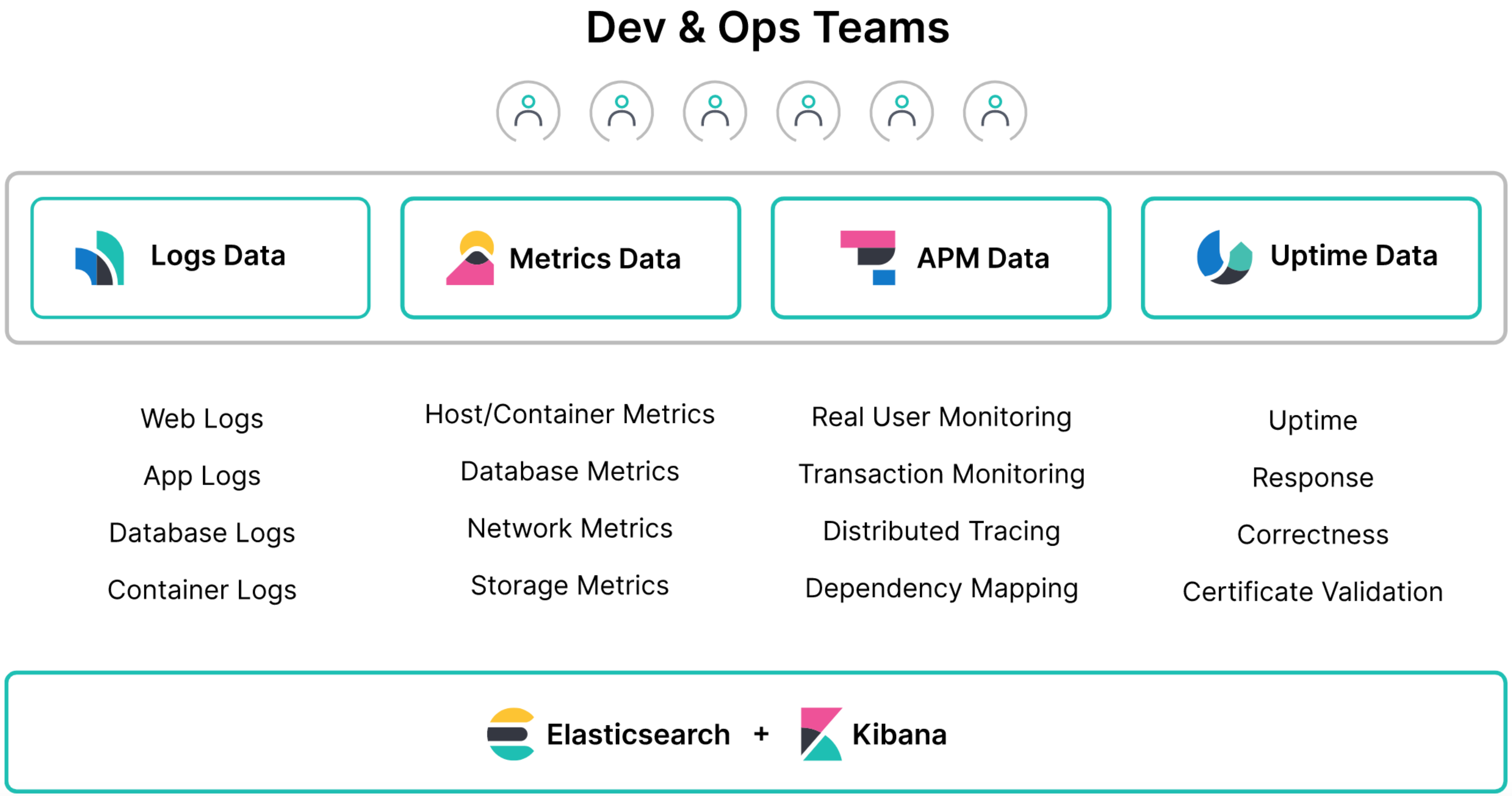
@timestamp
ecs_version
message

Group 2 (Must be populated to the max extent practical where event message contains relevant fields.)

Event	Device	Host	Agent	Network	Source	Destination	Service	Resource
event.category	device.mac	host.mac	agent.id	network.protocol	source.mac	destination.mac	service.id	resource.type
event.type	device.timezone_offset	host.timezone_offset	agent.name	network.forwarded_ip	source.ip	destination.ip	service.name	resource.id
event.data_source_id	device.ip	host.ip	agent.version	network.inbound_bytes	source.hostname	destination.hostname	service.version	resource.file_name
event.module	device.network_interface	host.network_interface		network.inbound_packets	source.domain	destination.domain	service.type	resource.uri
event.organization_name	device.hostname	host.hostname		network.outbound_bytes	source.port	destination.subdomain	service.state	resource.url
event.organization_id	device.type	host.id		network.outbound_packets		destination.port	service.query	resource.path
event.id	device.vendor	host.type		network.total_bytes			service.response_code	resource.version
event.raw	device.product	host.sub_type		network.total_packets				resource.hash_value
event.hash	device.version	host.operating_system		network.direction				resource.hash_type
event.tags	device.serial_number	host.operating_system_version						
event.labels	device.action	host.provider						
event.duration	device.rule_set	host.availability_zone						
event.severity	device.event_id	host.region						
event.risk_score								

ELASTIC STACK

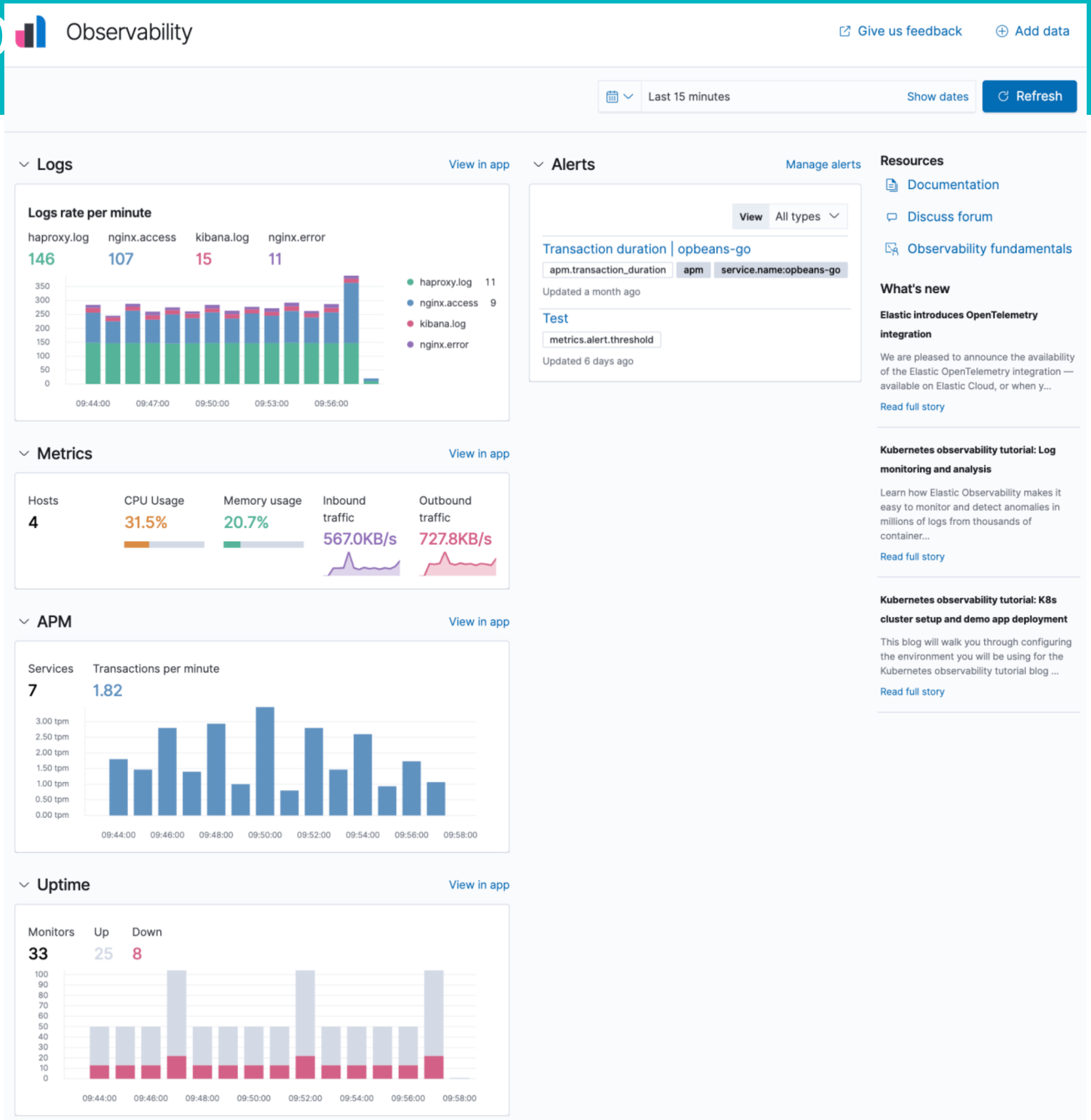
Acquisizione ed **elaborazione** di una grande mole di eventi **logs**, **metriche, tracce APM e monitoraggio** per avere il pieno controllo dell'**infrastruttura**.



OSW2021 OPENSOURCEWEEK

UNICA PIATTAFORMA DI OSSERVAZIO

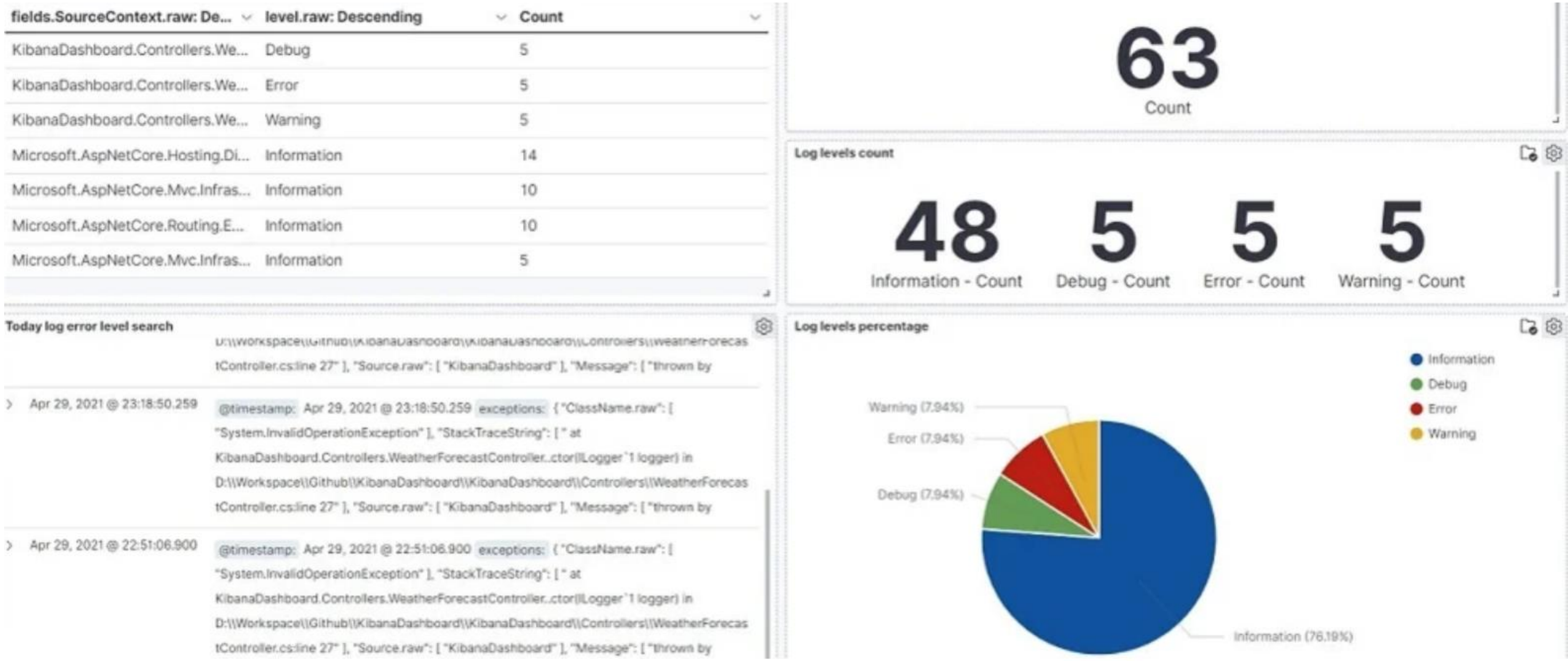
Grazie alla evoluzione di **Kibana** risulta possibile osservare l’intera infrastruttura da una **singola interfaccia**



OSW2021
OPENSOURCEWEEK

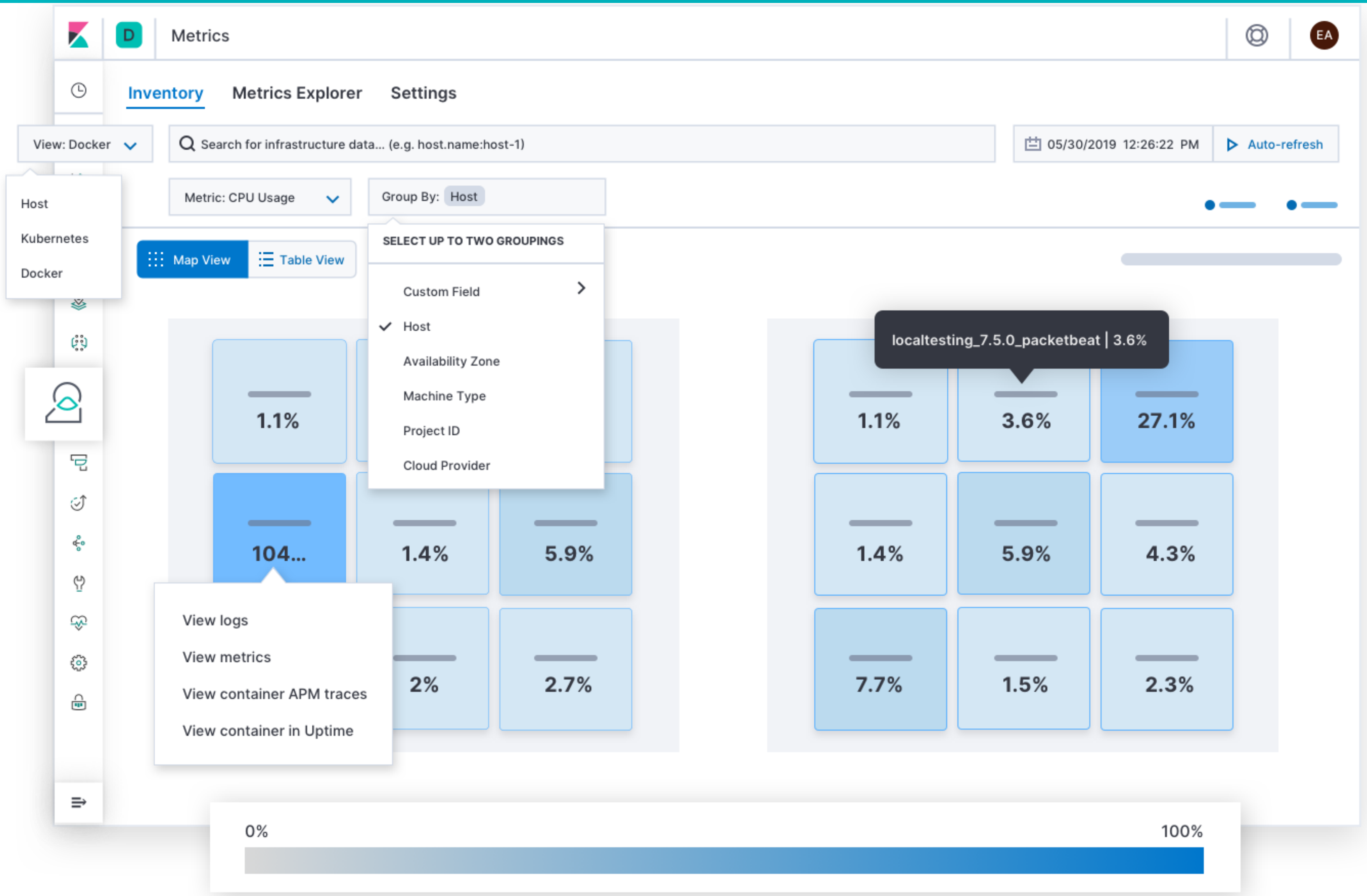
I LOG

Rappresentano la base di ogni soluzione di observability in termini di valore informativo e volumi.



LE METRICHE

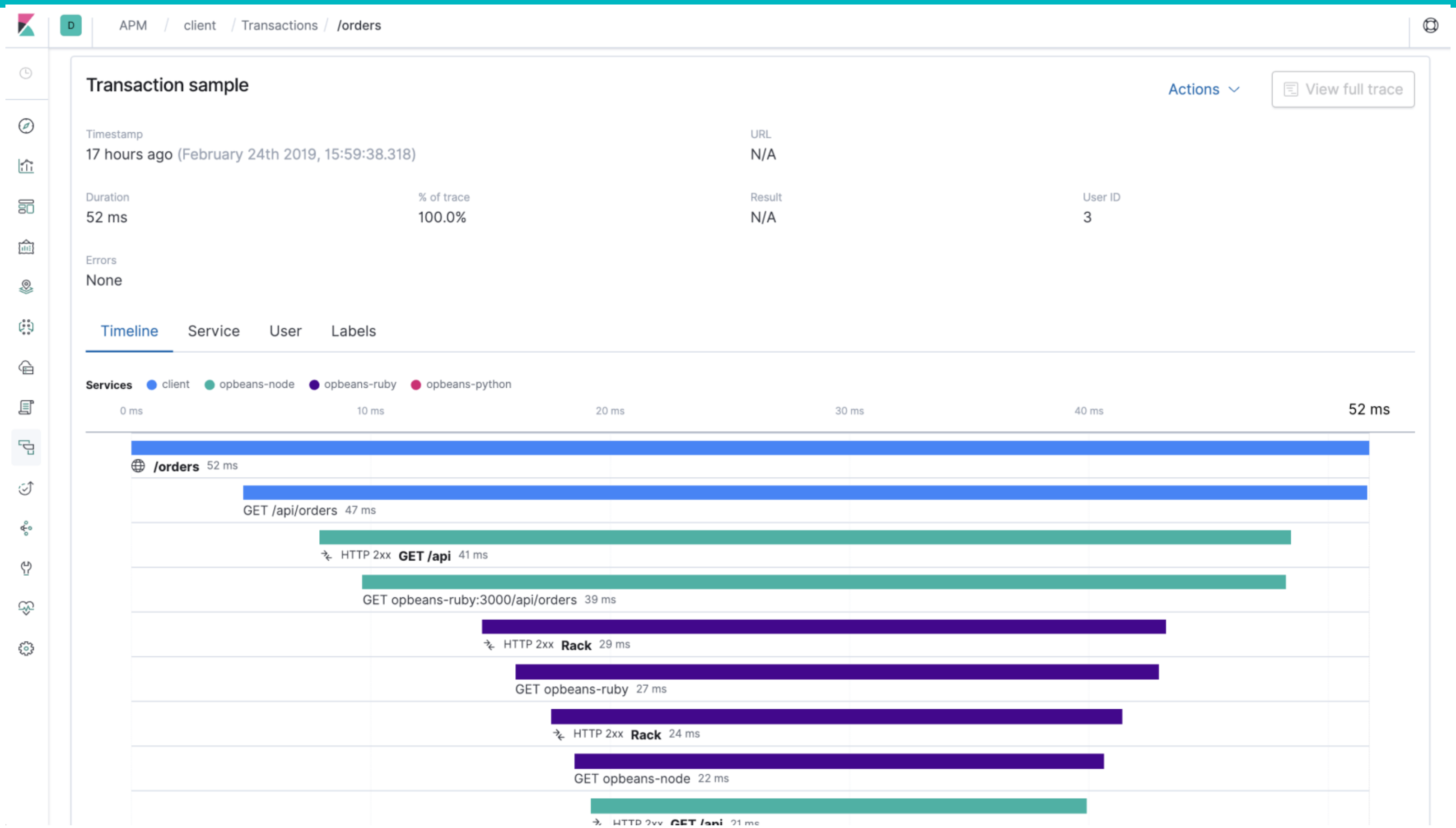
Quelle Applicative e di Infrastruttura si integrano con gli eventi di log ed incrementano la capacità di supervisione.



OSW2021 OPENSOURCEWEEK

I TRACCIATI

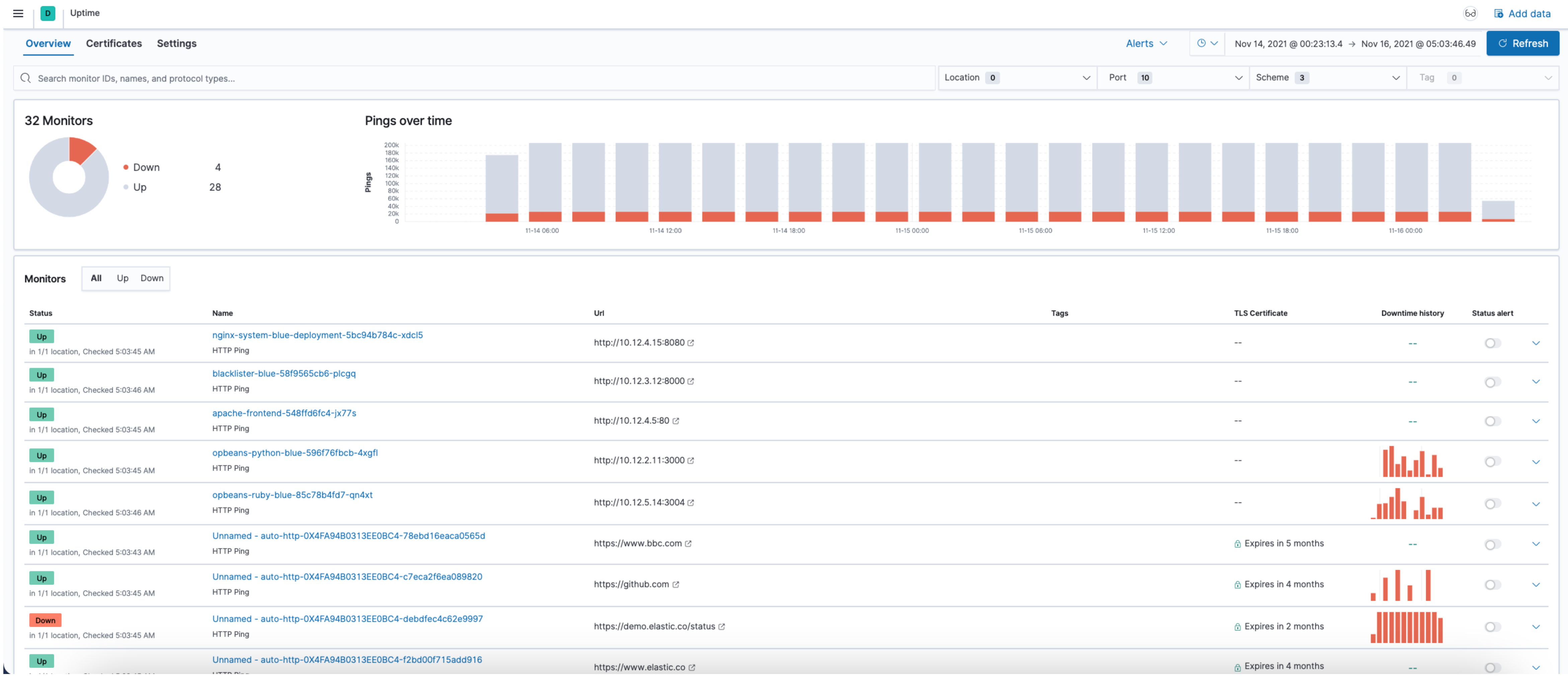
Grazie alla funzione APM risulta possibile tenere sotto controllo il funzionamento di applicazioni distribuite



OSW2021 OPENSOURCEWEEK

IL MONITORAGGIO

Visibilità dello stato dei servizi e loro raggiungibilità, verifica validità certificati



Compliance

COMPLIANCE

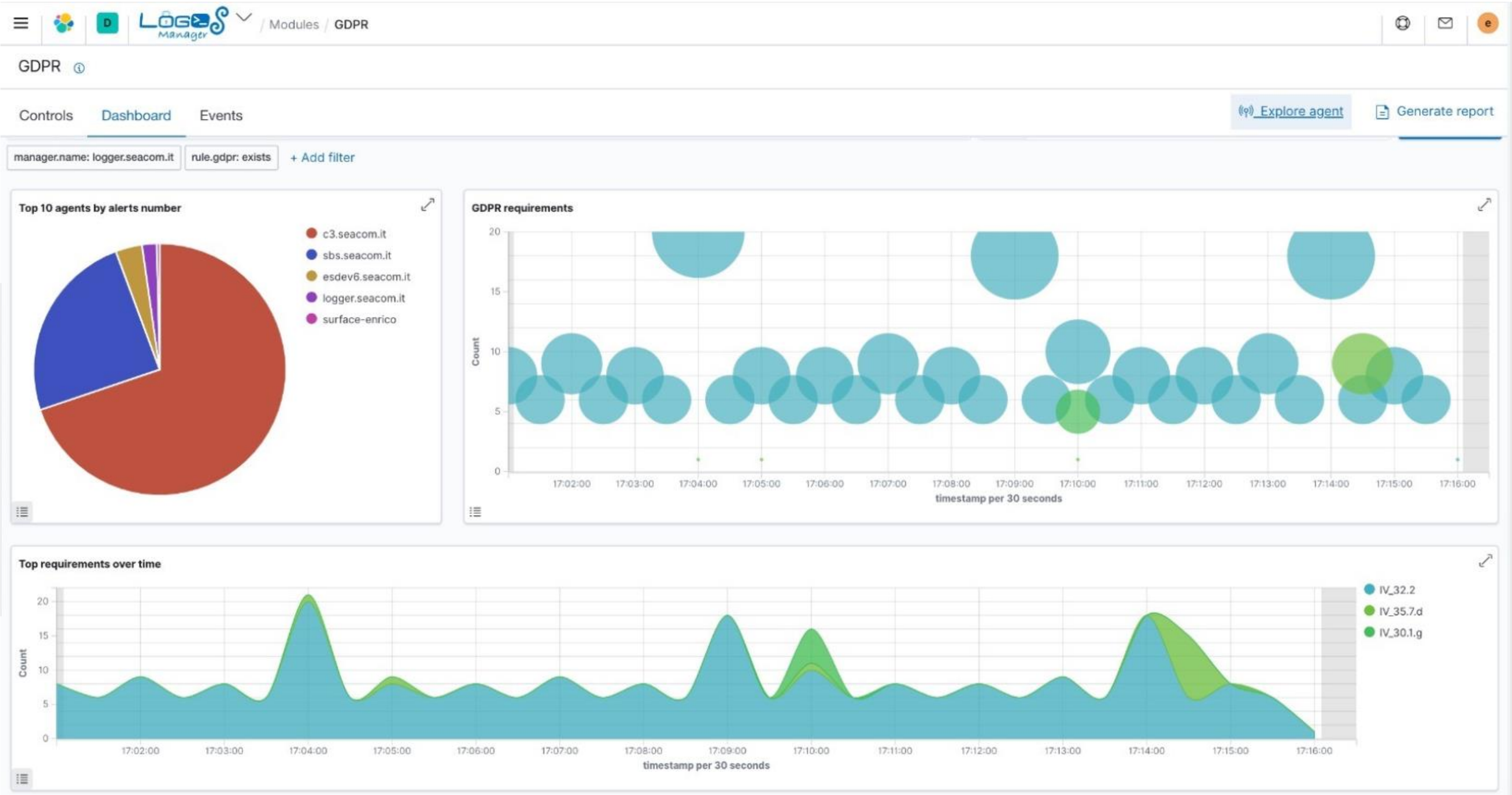
La nostra funzione modulare consente l’aggiunta della compliance direttamente sugli eventi acquisiti

Conservazione e inalterabilità - Raccogliere e conservare il dato garantendone **l’inalterabilità**. E’ possibile anche **attivare il meccanismo della marca temporale.**	**Security Analytics -** Raccogliere, aggregare, indicizzare e **analizzare i dati di sicurezza.**
File Integrity - Monitoraggio del file system su cambiamenti di contenuti, dei permessi, proprietà e attributi dei file. Identificazione nativa degli utenti e delle applicazioni utilizzare per creare o modificare file.	**Log Data Analysis -** Lettura e analisi dei LOG del SO e delle applicazioni: analizzati e archiviate in base a regole che permettono di evidenziare errori, configurazioni errate, attività dannose, violazioni della privacy, ecc.
Adozione di **appropriate politiche di protezione del dato da parte del titolare del trattamento** grazie a strumenti quali Rootcheck, OpenSCAP, CIS-CAT.	**Restringere su richieste del proprietario l'accesso al dato** grazie ad alert per accessi a file su cui siano richieste restrizioni

Regulatory Compliance - Controlli di sicurezza di conformità agli standard e alle normative di settore. Utilizzato dalle società di elaborazione dei pagamenti/istituzioni finanziarie per soddisfare i requisiti GDPR, PCI DSS (Payment Card Industry Data Security Standard).

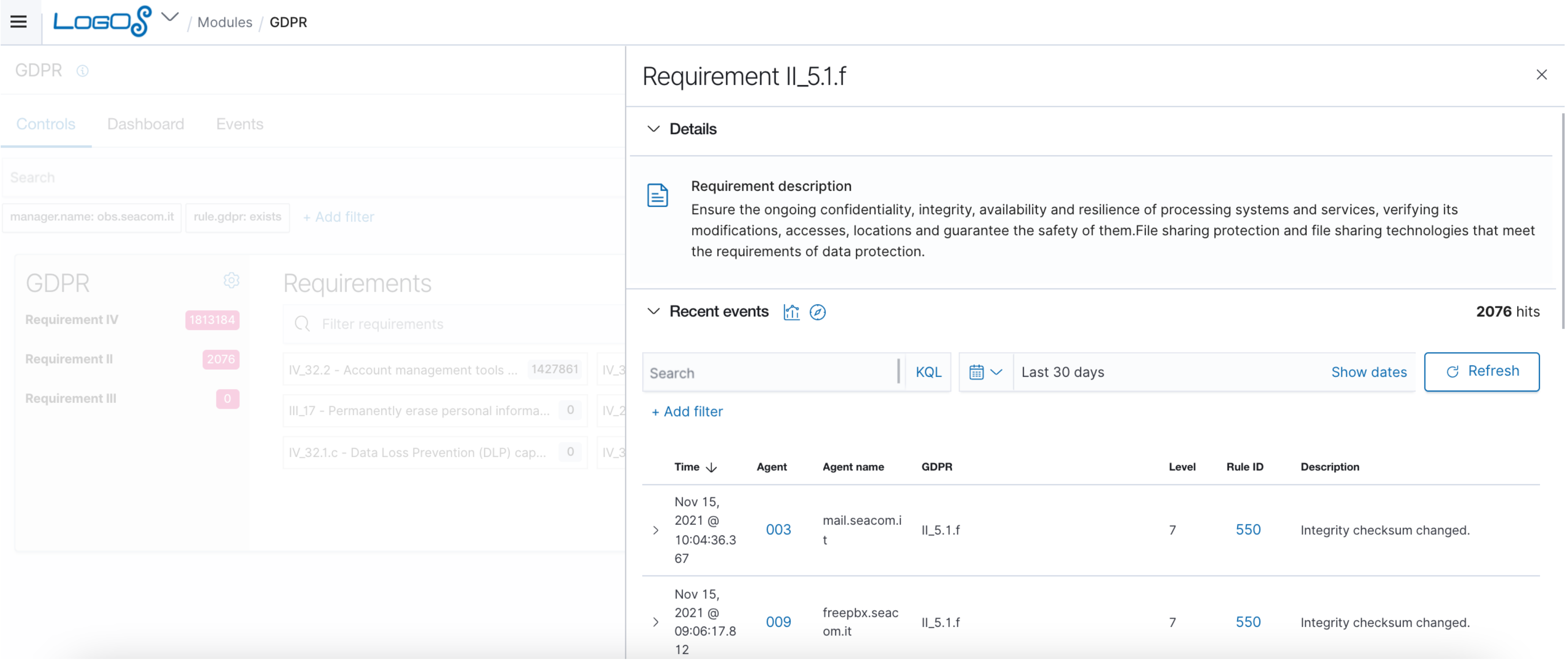
COMPLIANCE

Tutte le funzionalità di analisi sono fruibili dalla stessa interfaccia



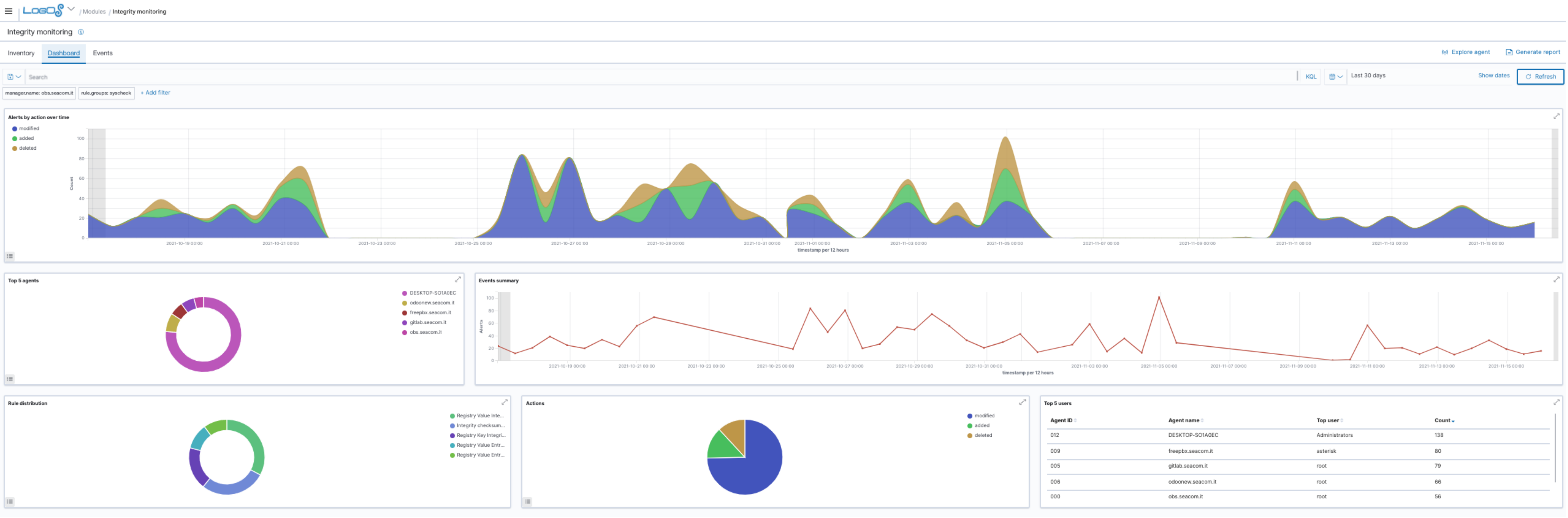
COMPLIANCE

Dashboard di investigazione dei requisiti delle varie normative



COMPLIANCE - FIM

Controllo costante dell’Integrtità dei sistemi

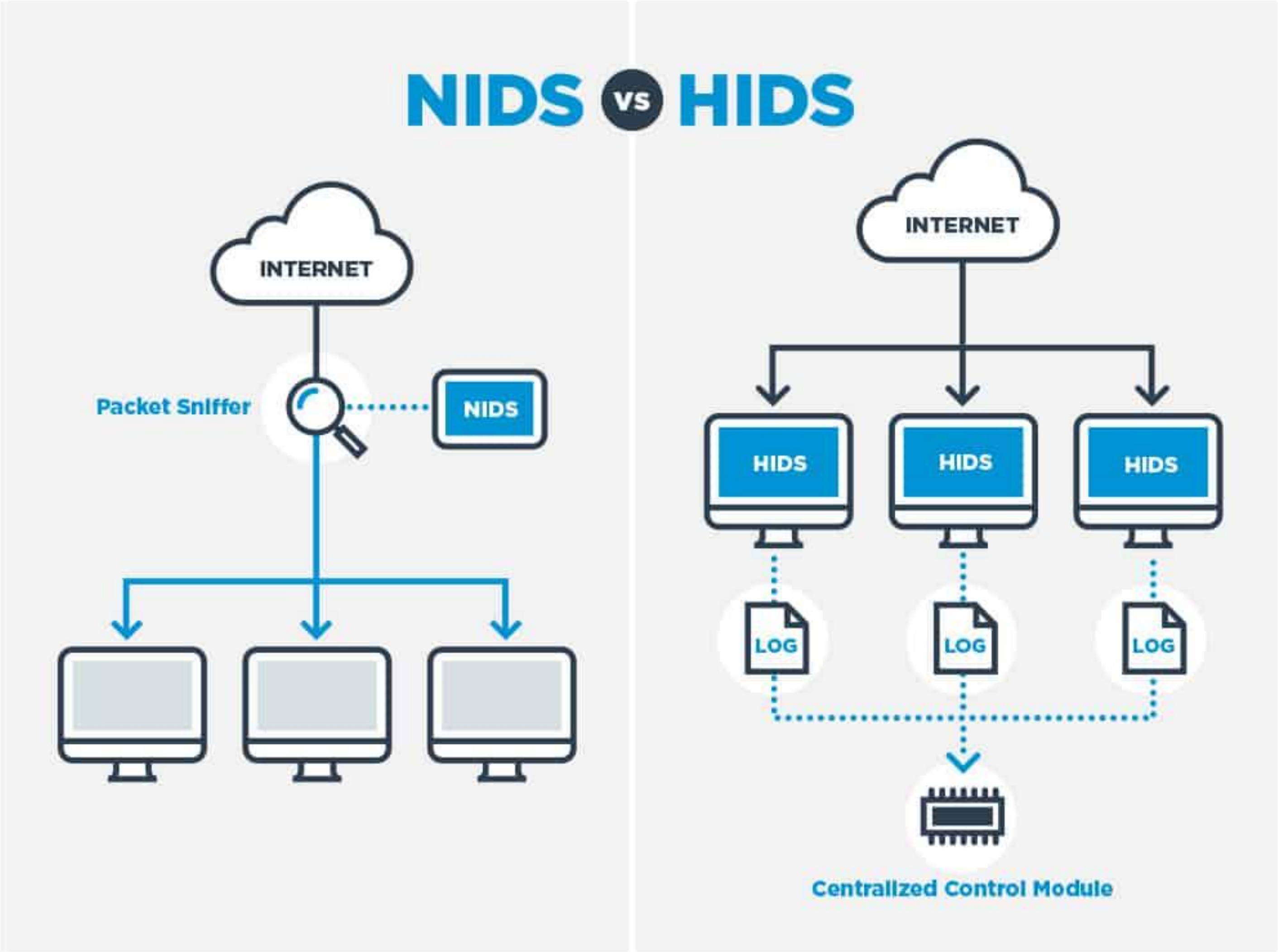


OSW2021 OPENSOURCEWEEK

Security

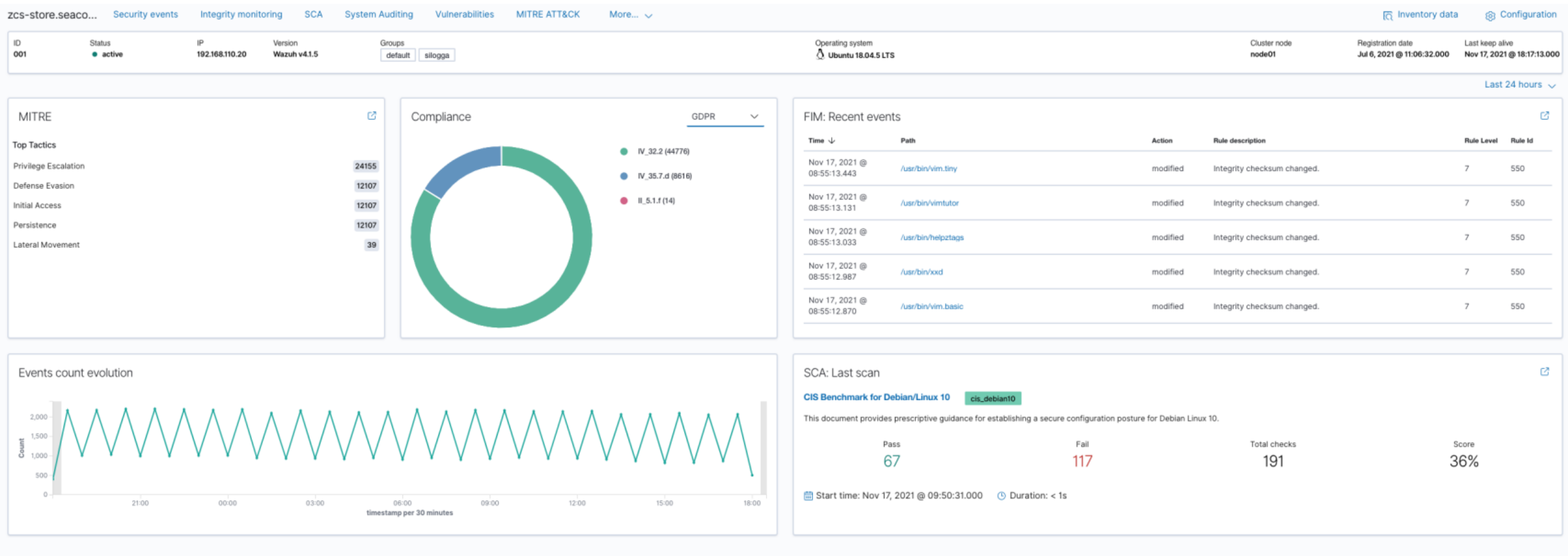
RIOS RETE ITALIANA OPEN SOURCE

LE SONDE


NIDS vs HIDS
INTERNET
Packet Sniffer
NIDS
INTERNET
HIDS
HIDS
HIDS
LOG
LOG
LOG
Centralized Control Module

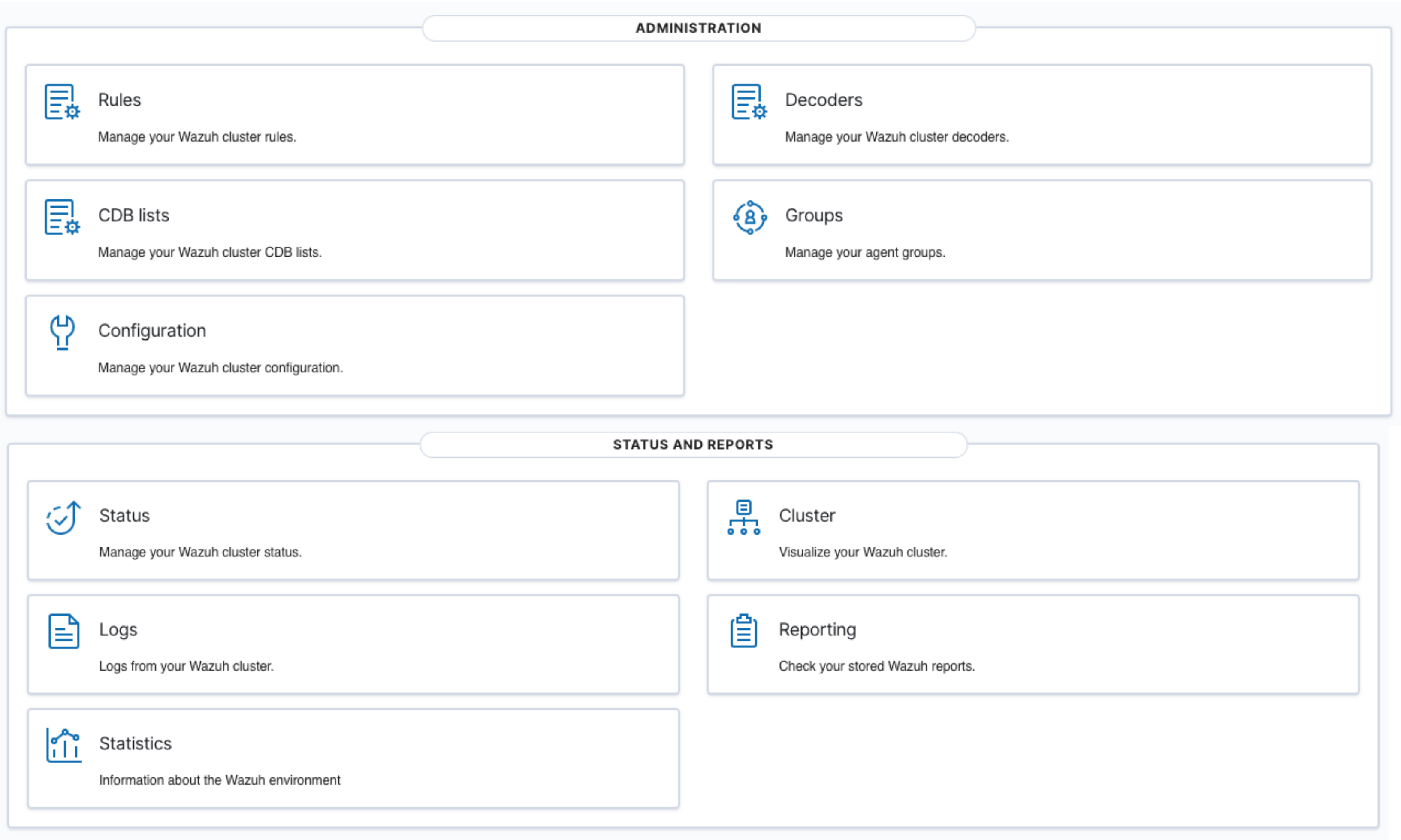
LE FUNZIONI SIEM

- Rilevazione delle Vulnerabilità
- Rilevazione Malware
- Identificazione Code Injection
- Security Configuration Assessment
- Audit di Sistema
- Monitoraggio Policy
- Allarmi webhook
- Allarmi ML
- Sicurezza Cloud
- Active Response

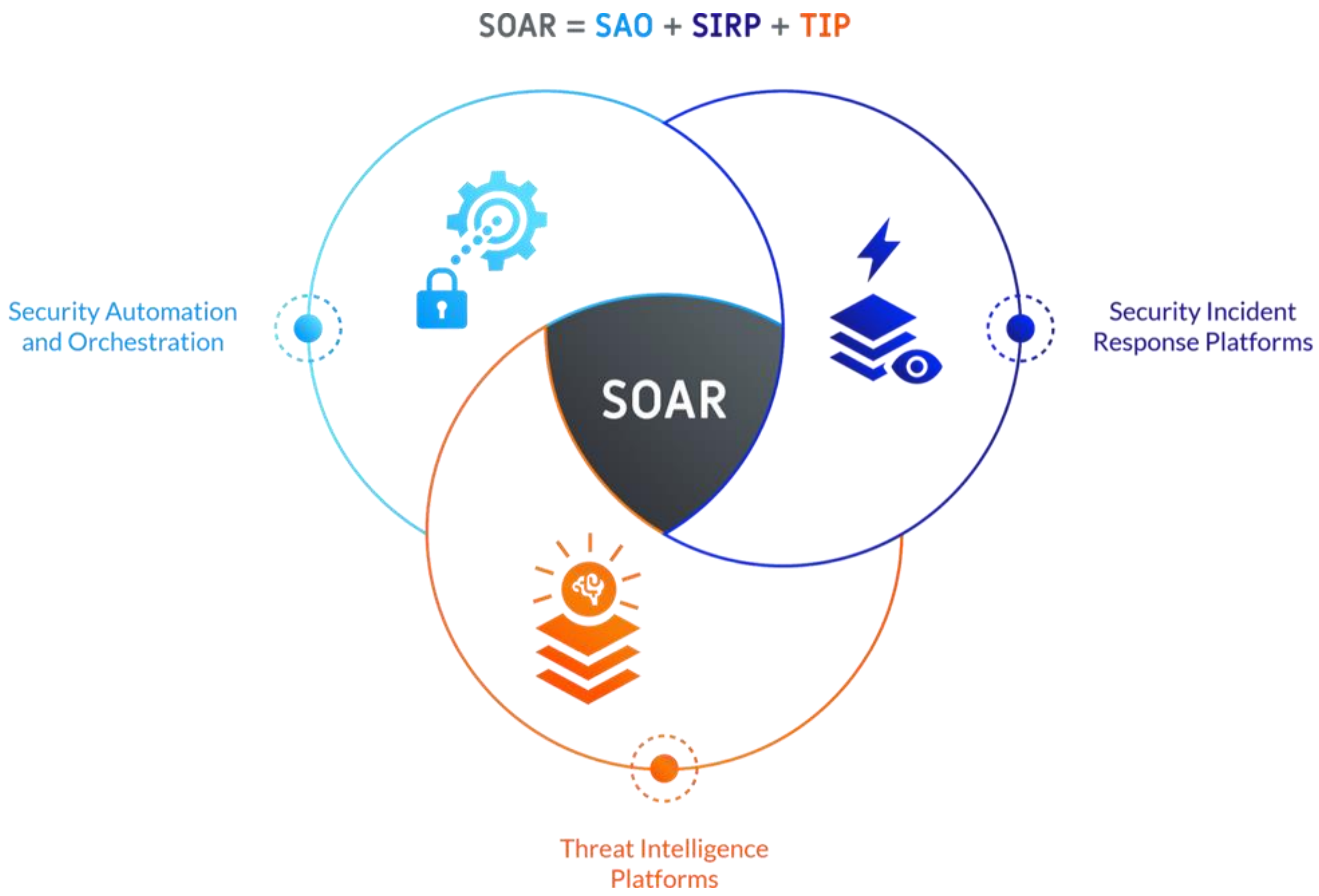


LA GESTIONE CENTRALIZZATA

- Configurazione sonde HIDS NIDS
- Configurazione SIEM rule/decoder
- CDB List
- Reportistica
- Monitoraggio

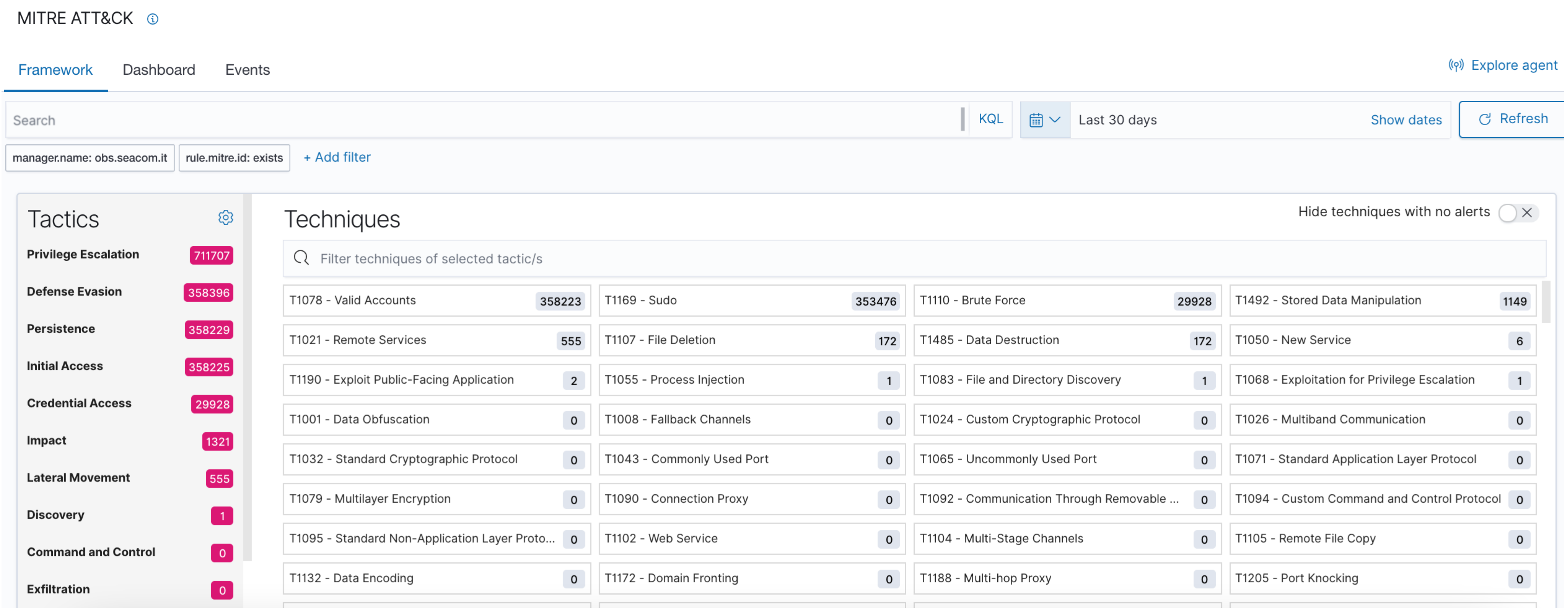


LE INTEGRAZIONI



TIP – MITRE ATT&CK

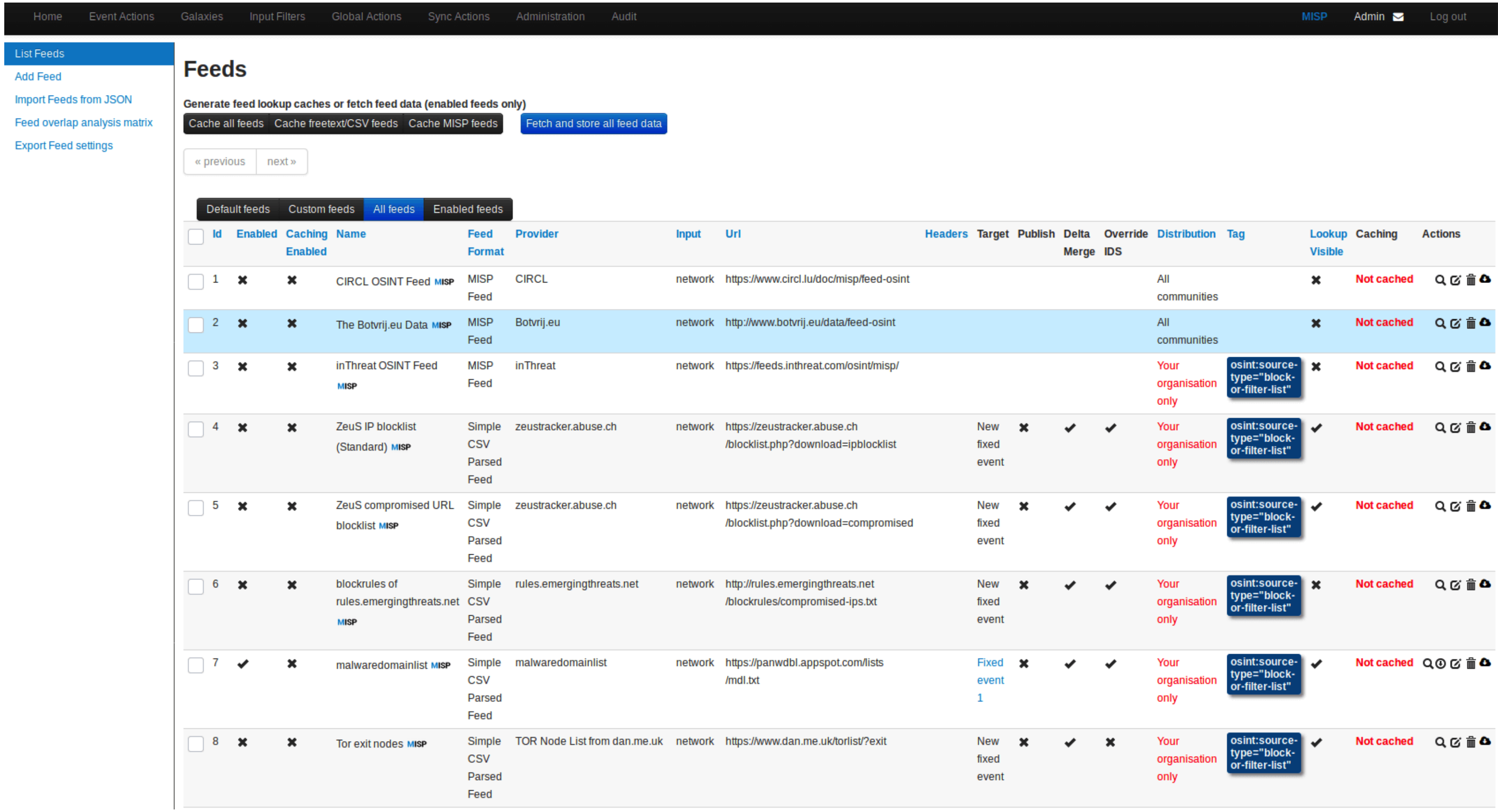
Analisi Tecniche/Tattiche di attacco grazie alla classificazione Mitre ATT&CK



TIP – MISP

Integrazione IOC MISP

- Indirizzi IP
- Domini
- URL
- File hash
- Email
- ….



Home | Event Actions | Galaxies | Input Filters | Global Actions | Sync Actions | Administration | Audit | MISP | Admin | Log out

- List Feeds
- Add Feed
- Import Feeds from JSON
- Feed overlap analysis matrix
- Export Feed settings

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Cache all feeds | Cache freetext/CSV feeds | Cache MISP feeds | Fetch and store all feed data

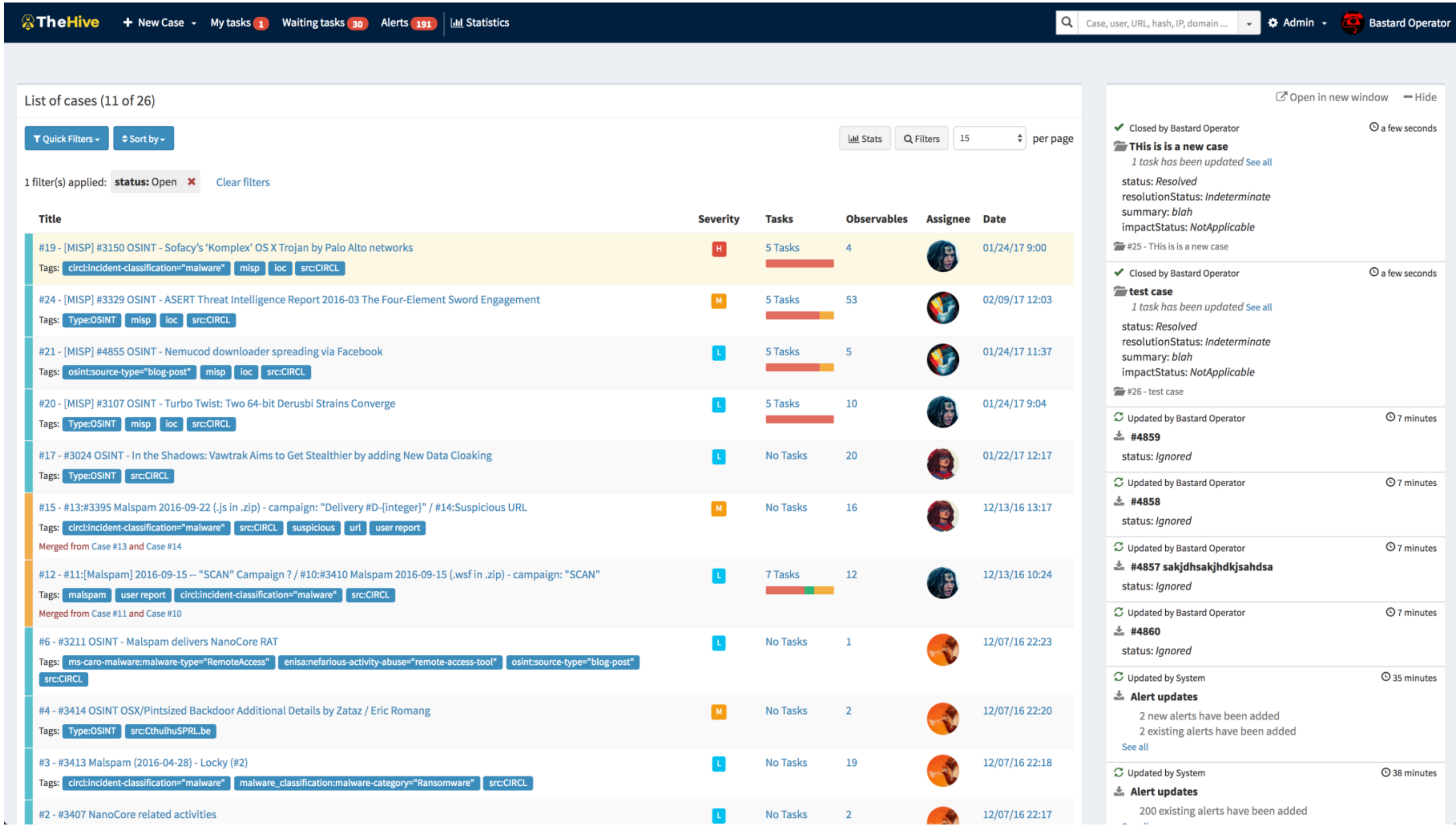
« previous | next »

Default feeds | Custom feeds | All feeds | Enabled feeds

Id	Enabled	Caching Enabled	Name	Feed Format	Provider	Input	Url	Headers	Target	Publish	Delta Merge	Override IDS	Distribution	Tag	Lookup Visible	Caching	Actions
1	✖	✖	CIRCL OSINT Feed MISP	MISP Feed	CIRCL	network	https://www.circl.lu/doc/misp/feed-osint						All communities		✖	Not cached	
2	✖	✖	The Botvrij.eu Data MISP	MISP Feed	Botvrij.eu	network	http://www.botvrij.eu/data/feed-osint						All communities		✖	Not cached	
3	✖	✖	inThreat OSINT Feed MISP	MISP Feed	inThreat	network	https://feeds.inthreat.com/osint/misp/						Your organisation only	osint:source-type="block-or-filter-list"	✖	Not cached	
4	✖	✖	ZeuS IP blocklist (Standard) MISP	Simple CSV Parsed Feed	zeustracker.abuse.ch	network	https://zeustracker.abuse.ch /blocklist.php?download=ipblocklist		New fixed event	✖	✔	✔	Your organisation only	osint:source-type="block-or-filter-list"	✔	Not cached	
5	✖	✖	ZeuS compromised URL blocklist MISP	Simple CSV Parsed Feed	zeustracker.abuse.ch	network	https://zeustracker.abuse.ch /blocklist.php?download=compromised		New fixed event	✖	✔	✔	Your organisation only	osint:source-type="block-or-filter-list"	✔	Not cached	
6	✖	✖	blockrules of rules.emergingthreats.net MISP	Simple CSV Parsed Feed	rules.emergingthreats.net	network	http://rules.emergingthreats.net /blockrules/compromised-ips.txt		New fixed event	✖	✔	✔	Your organisation only	osint:source-type="block-or-filter-list"	✖	Not cached	
7	✔	✖	malwaredomainlist MISP	Simple CSV Parsed Feed	malwaredomainlist	network	https://panwdbl.appspot.com/lists /mdl.txt		Fixed event 1	✖	✔	✔	Your organisation only	osint:source-type="block-or-filter-list"	✔	Not cached	
8	✖	✖	Tor exit nodes MISP	Simple CSV Parsed Feed	TOR Node List from dan.me.uk	network	https://www.dan.me.uk/torlist/?exit		New fixed event	✖	✔	✖	Your organisation only	osint:source-type="block-or-filter-list"	✔	Not cached	

SIRP – TheHive & Cortex

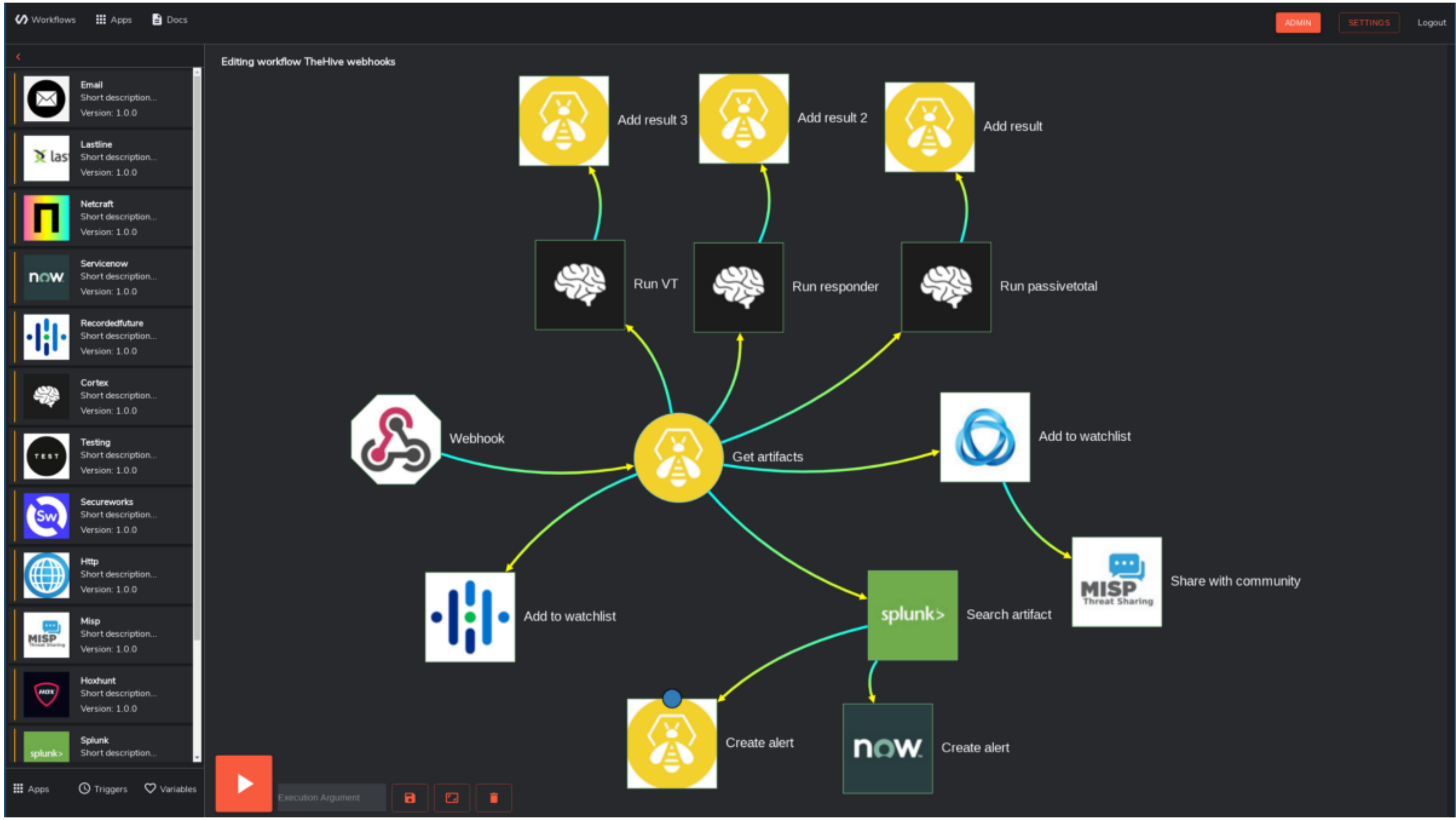
Integrato con MISP garantisce un ottima capacità di gestione degli incidenti di sicurezza provenienti dal SIEM



OSW2021 OPENSOURCEWEEK

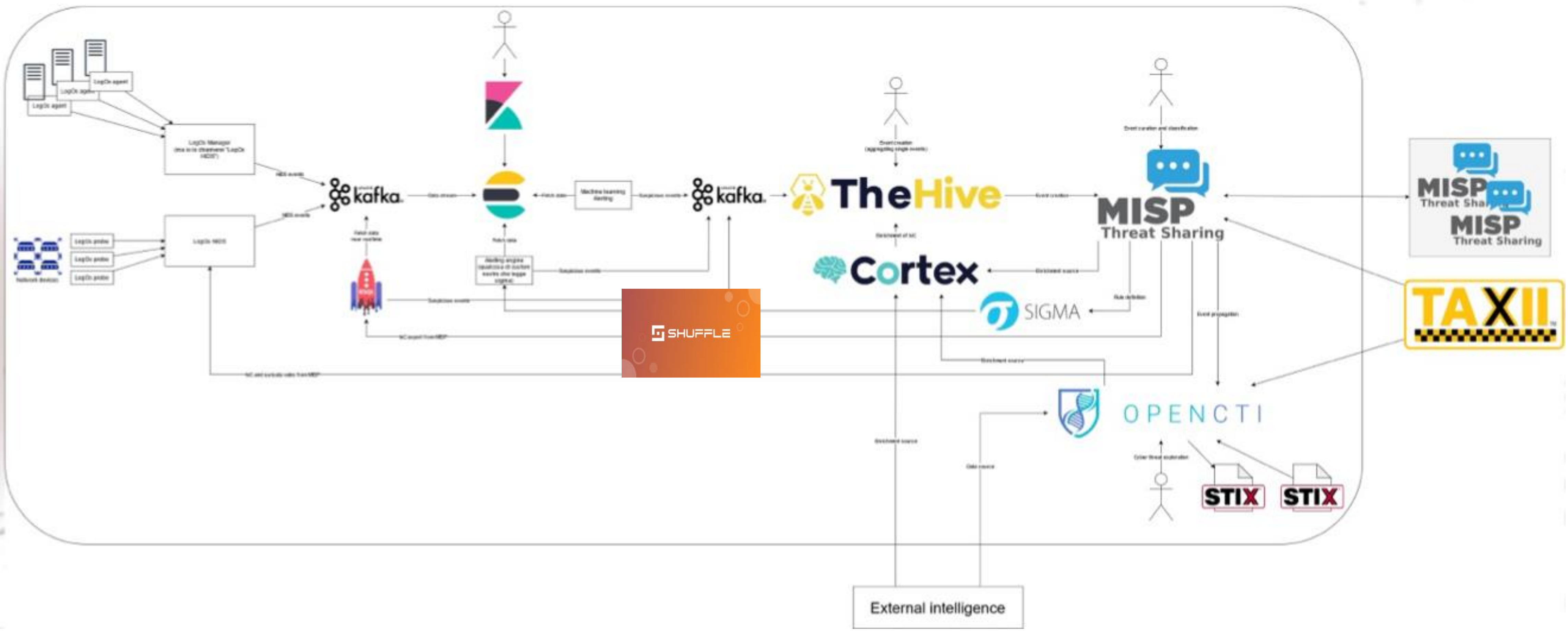
SOAR – Shuffle

Grazie a Shuffle risulta possibile disegnare dei processi di orchestrazione delle soluzioni di sicurezza.



Stack Completo

HLD


kafka
kafka
TheHive
MISP
Threat Sharing
MISP
Threat Sharing
MISP
Threat Sharing
Cortex
SIGMA
SHUFFLE
TAXII
OPENCTI
STIX
STIX
External intelligence

OSW2021
OPENSOURCEWEEK

BinarioEtico

eLabor
impariamo lavorando

Geobeyond

ITSERVICE-NET

LARUS

REDTURTLE
agile.open.connected

S2S

SEACOM

SMC