



Una piattaforma unificata di Observability, Compliance e Security

Alessandro Fortunati
CTO @ Seacom

#OSW2021



RETE ITALIANA
OPEN SOURCE



Observability



RETE ITALIANA
OPEN SOURCE

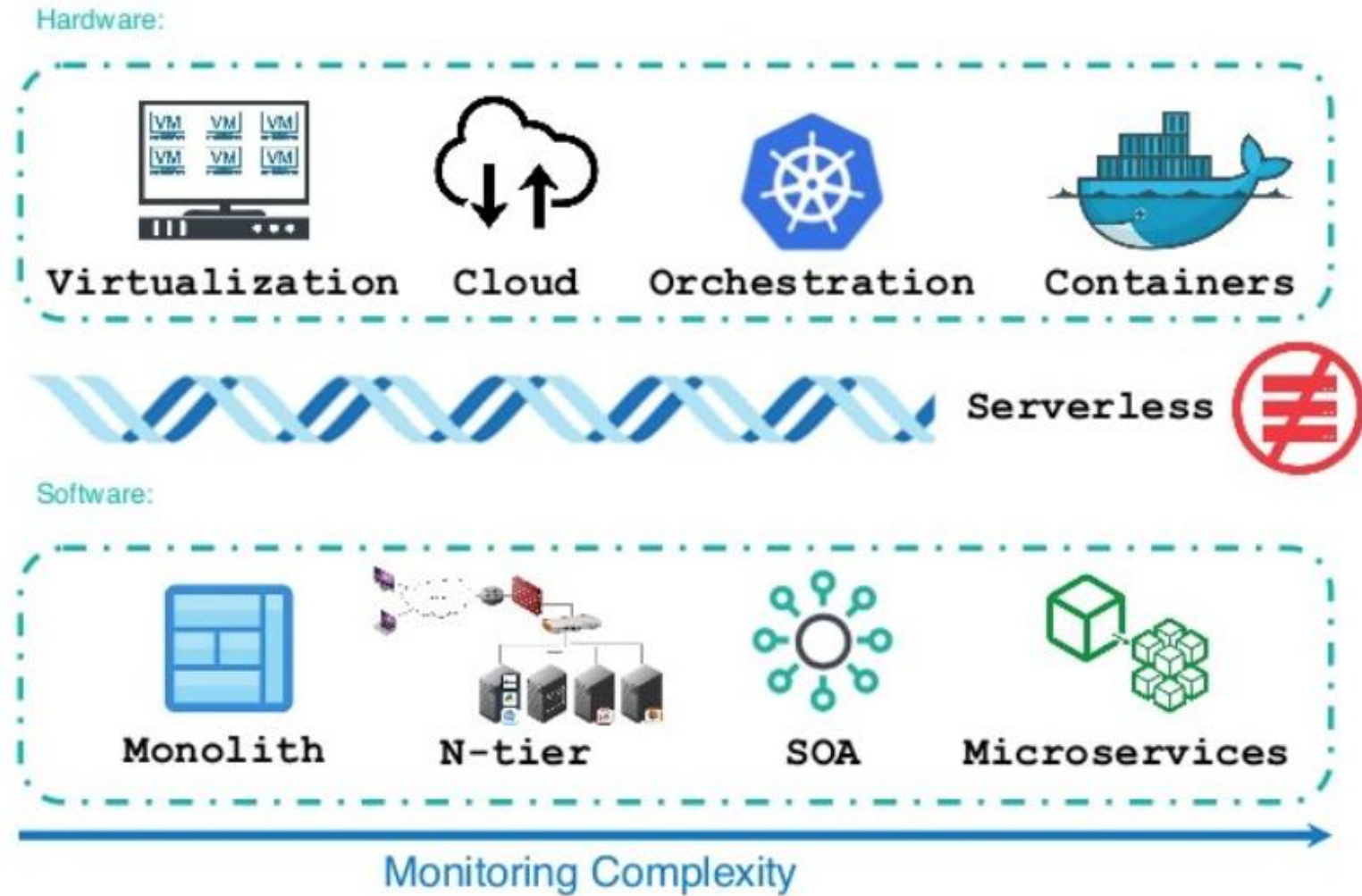
OSSERVABILITA'

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



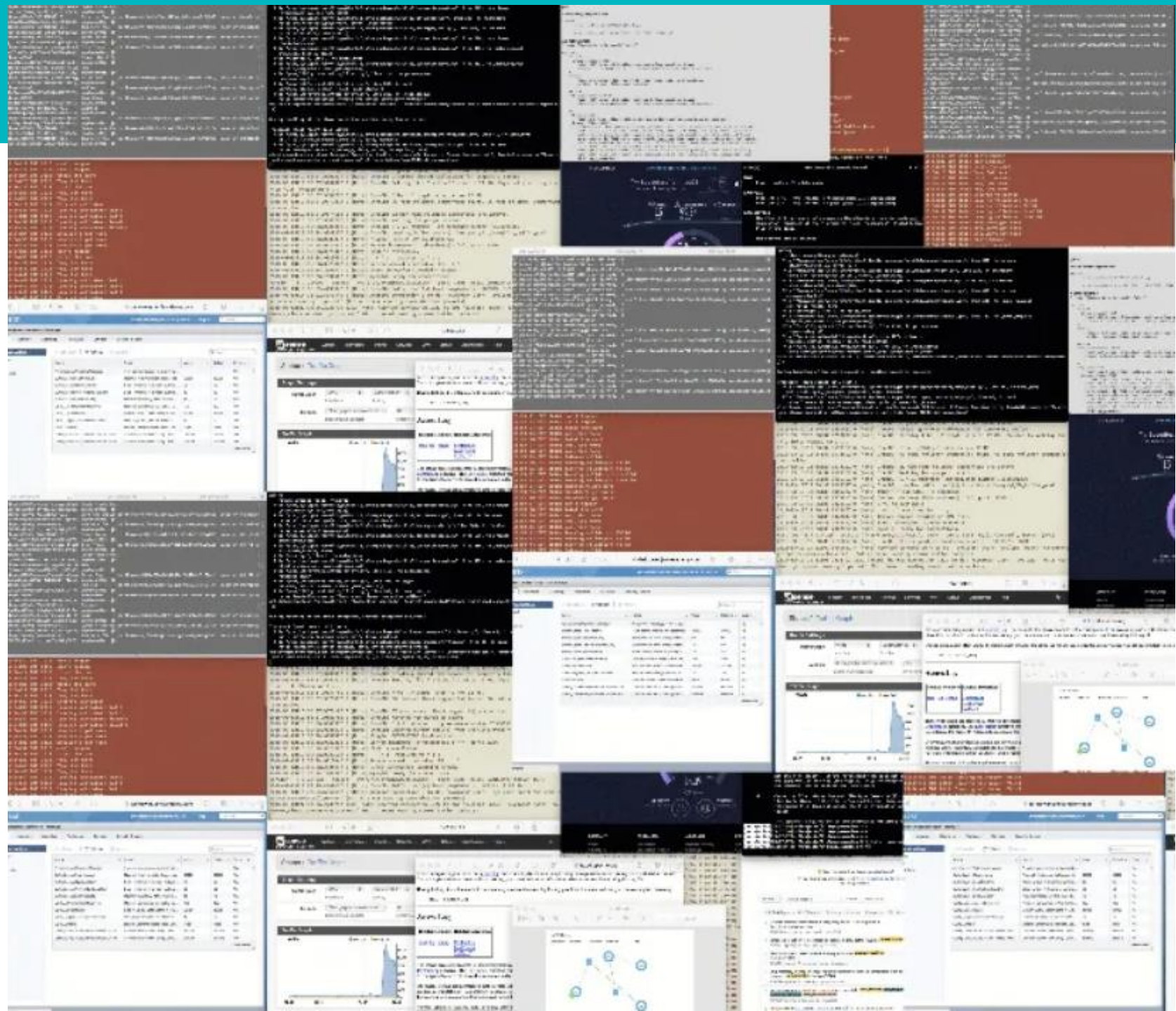
ARCHITETTURE IN EVOLUZIONE

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



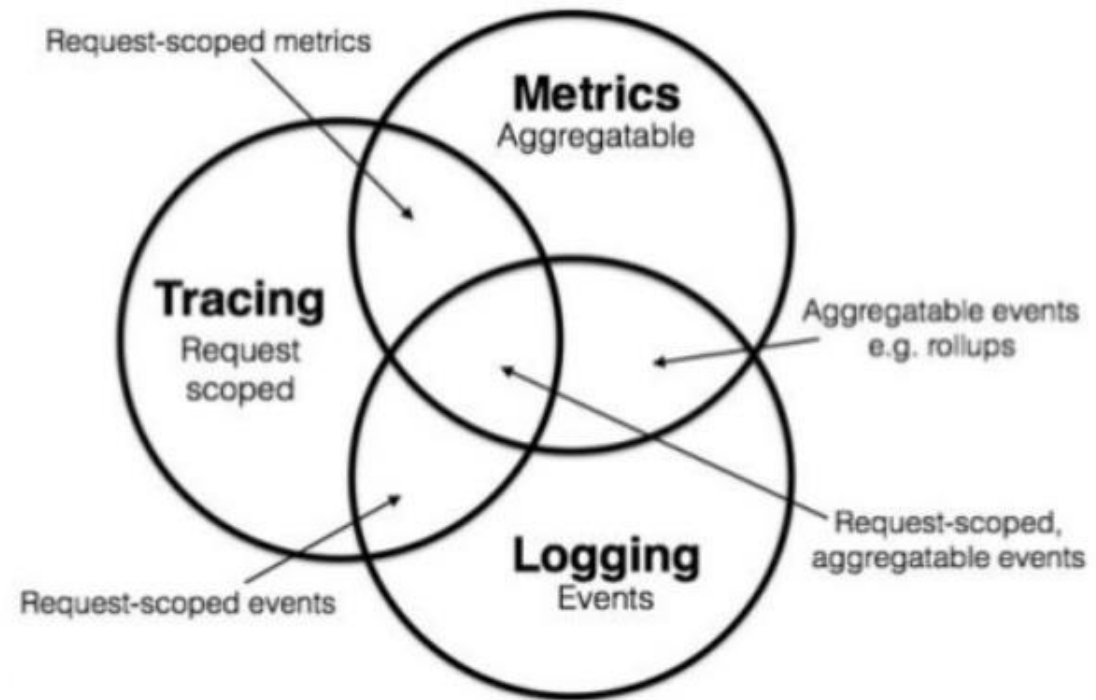
LA DISPERSIONE

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**



I PILASTRI

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



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.

Dev & Ops Teams



Logs Data



Metrics Data



APM Data



Uptime Data

Web Logs

App Logs

Database Logs

Container Logs

Host/Container Metrics

Database Metrics

Network Metrics

Storage Metrics

Real User Monitoring

Transaction Monitoring

Distributed Tracing

Dependency Mapping

Uptime

Response

Correctness

Certificate Validation



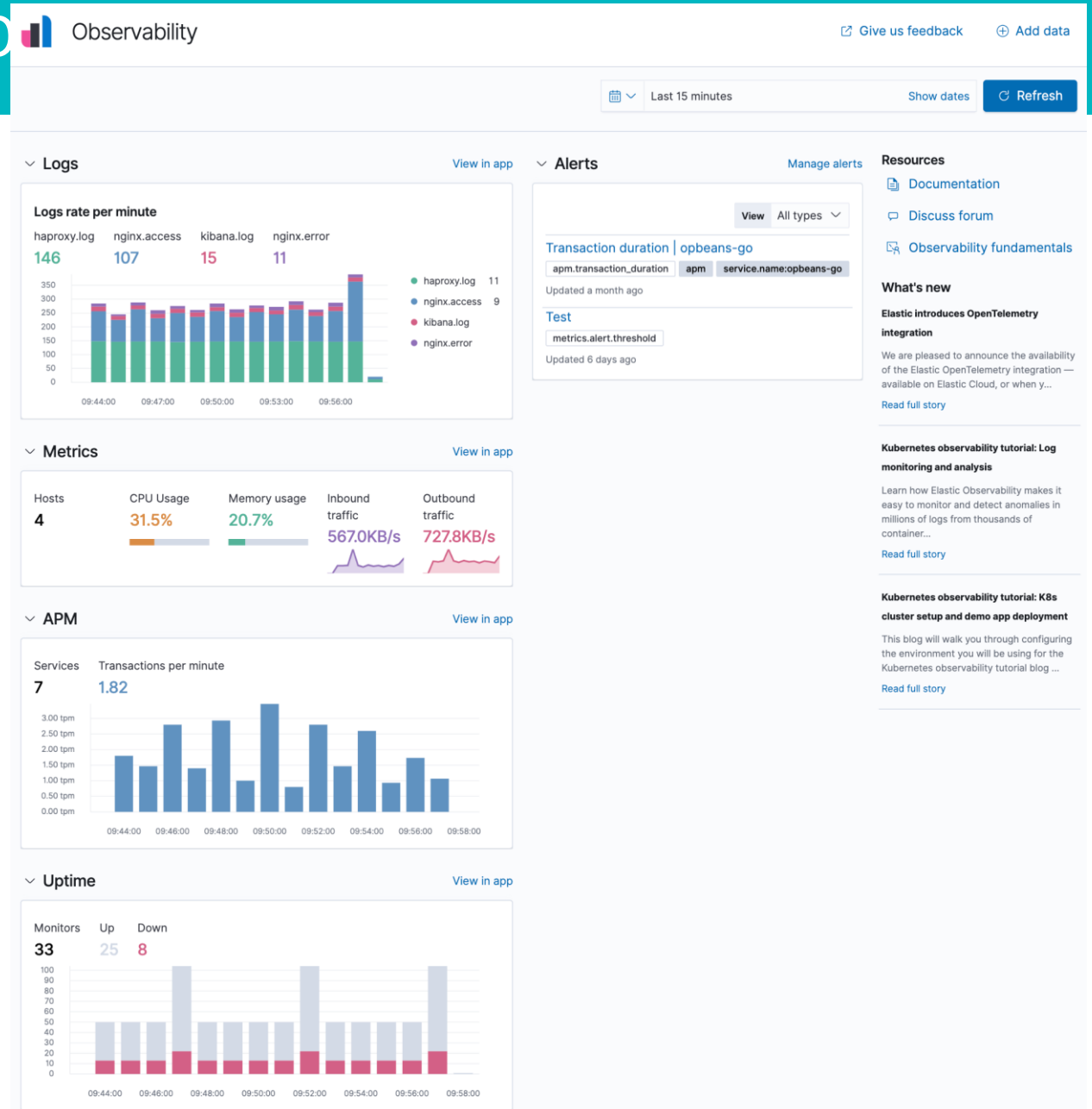
Elasticsearch +



Kibana

UNICA PIATTAFORMA DI OSSERVAZIONE

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

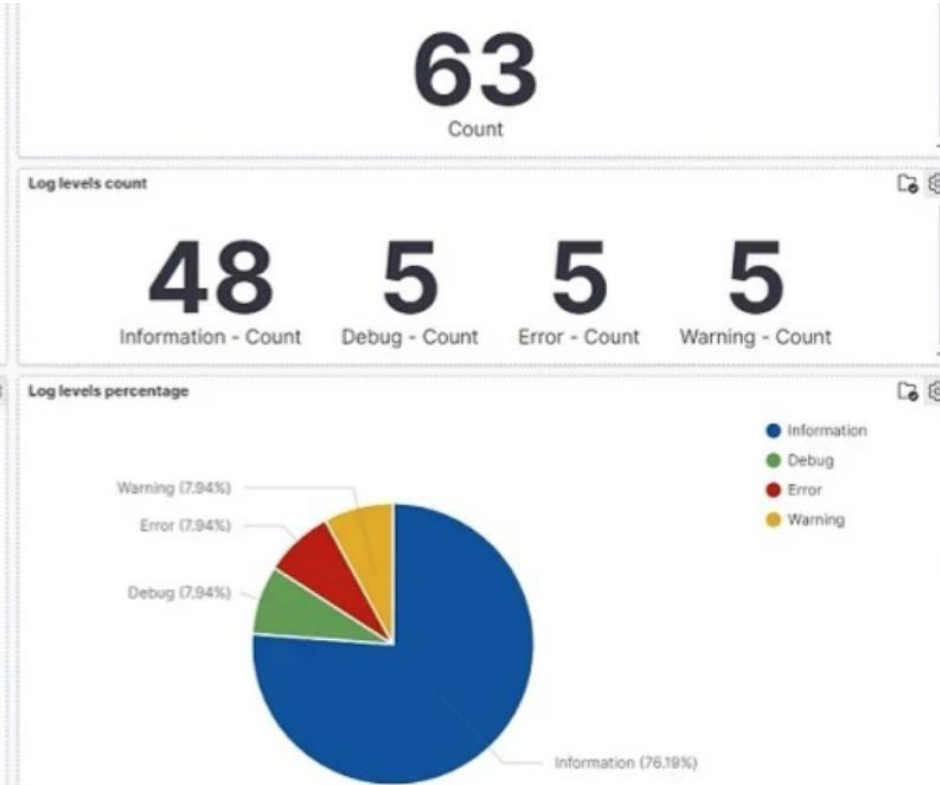


I LOG

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

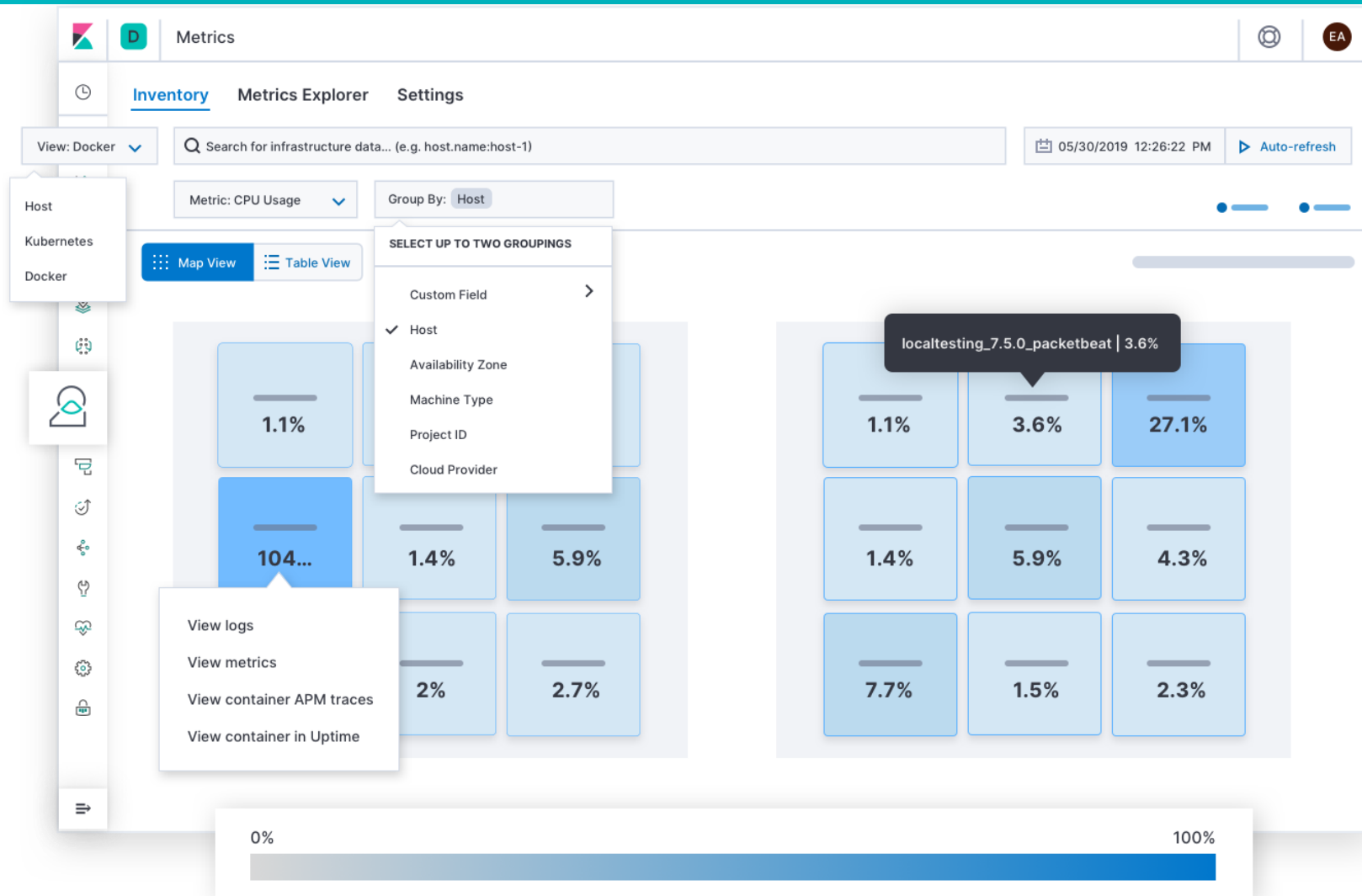
fields.SourceContext.raw: De...	level.raw: Descending	Count
KibanaDashboard.Controllers.We...	Debug	5
KibanaDashboard.Controllers.We...	Error	5
KibanaDashboard.Controllers.We...	Warning	5
Microsoft.AspNetCore.Hosting.Di...	Information	14
Microsoft.AspNetCore.Mvc.Infras...	Information	10
Microsoft.AspNetCore.Routing.E...	Information	10
Microsoft.AspNetCore.Mvc.Infras...	Information	5

Today log error level search	
> Apr 29, 2021 @ 23:18:50.259	@timestamp: Apr 29, 2021 @ 23:18:50.259 exceptions: { "ClassName.raw": ["System.InvalidOperationException"], "StackTraceString": [" at KibanaDashboard.Controllers.WeatherForecastController..ctor(ILogger`1 logger) in D:\\Workspace\\Github\\KibanaDashboard\\KibanaDashboard\\Controllers\\WeatherForecastController.cs:line 27"], "Source.raw": ["KibanaDashboard"], "Message": ["thrown by"] }
> Apr 29, 2021 @ 22:51:06.900	@timestamp: Apr 29, 2021 @ 22:51:06.900 exceptions: { "ClassName.raw": ["System.InvalidOperationException"], "StackTraceString": [" at KibanaDashboard.Controllers.WeatherForecastController..ctor(ILogger`1 logger) in D:\\Workspace\\Github\\KibanaDashboard\\KibanaDashboard\\Controllers\\WeatherForecastController.cs:line 27"], "Source.raw": ["KibanaDashboard"], "Message": ["thrown by"] }



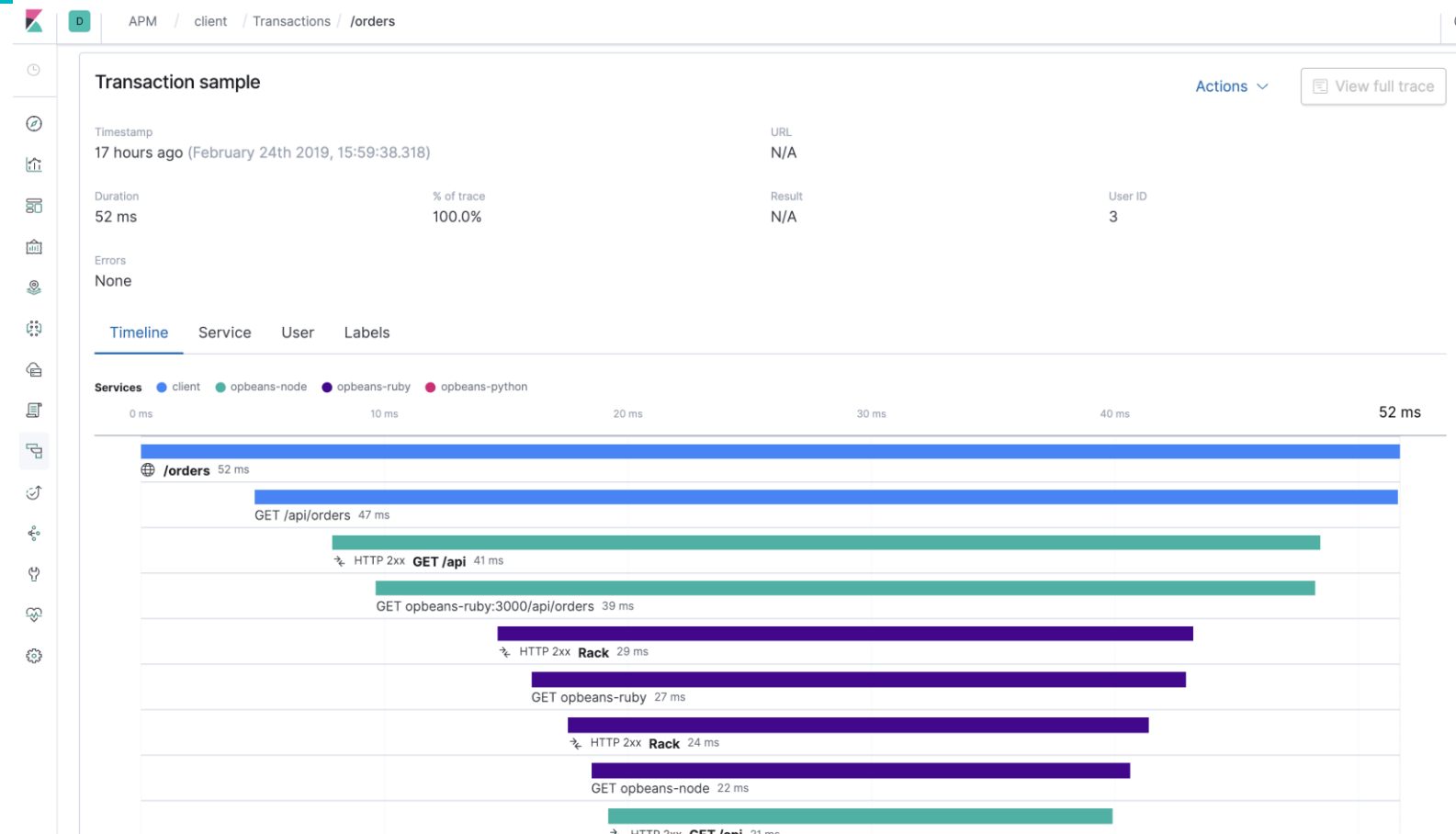
LE METRICHE

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

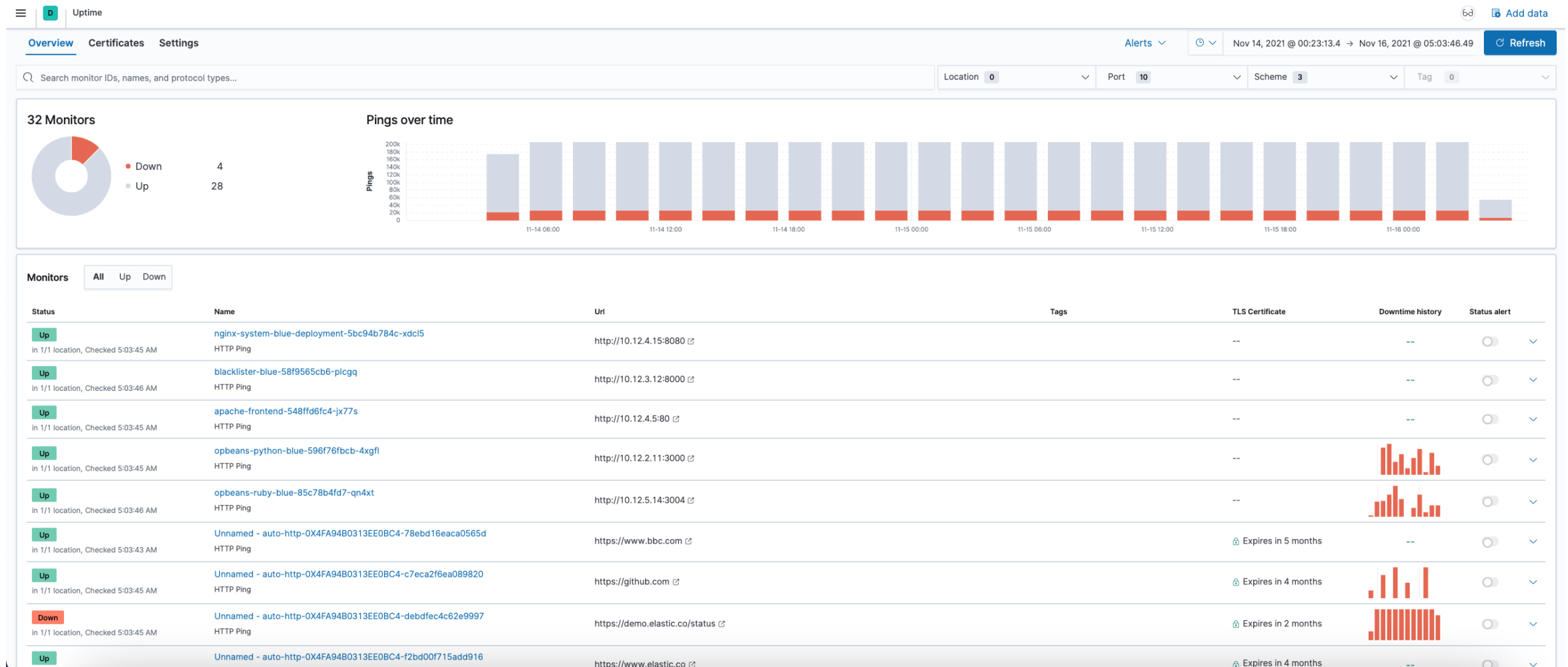


I TRACCIATI

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



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





Compliance



RETE ITALIANA
OPEN SOURCE

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**.

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.

Adozione di **appropriate politiche di protezione del dato da parte del titolare del trattamento** grazie a strumenti quali Rootcheck, OpenSCAP, CIS-CAT.

Security Analytics - Raccogliere, aggregare, indicizzare e **analizzare i dati di sicurezza**.

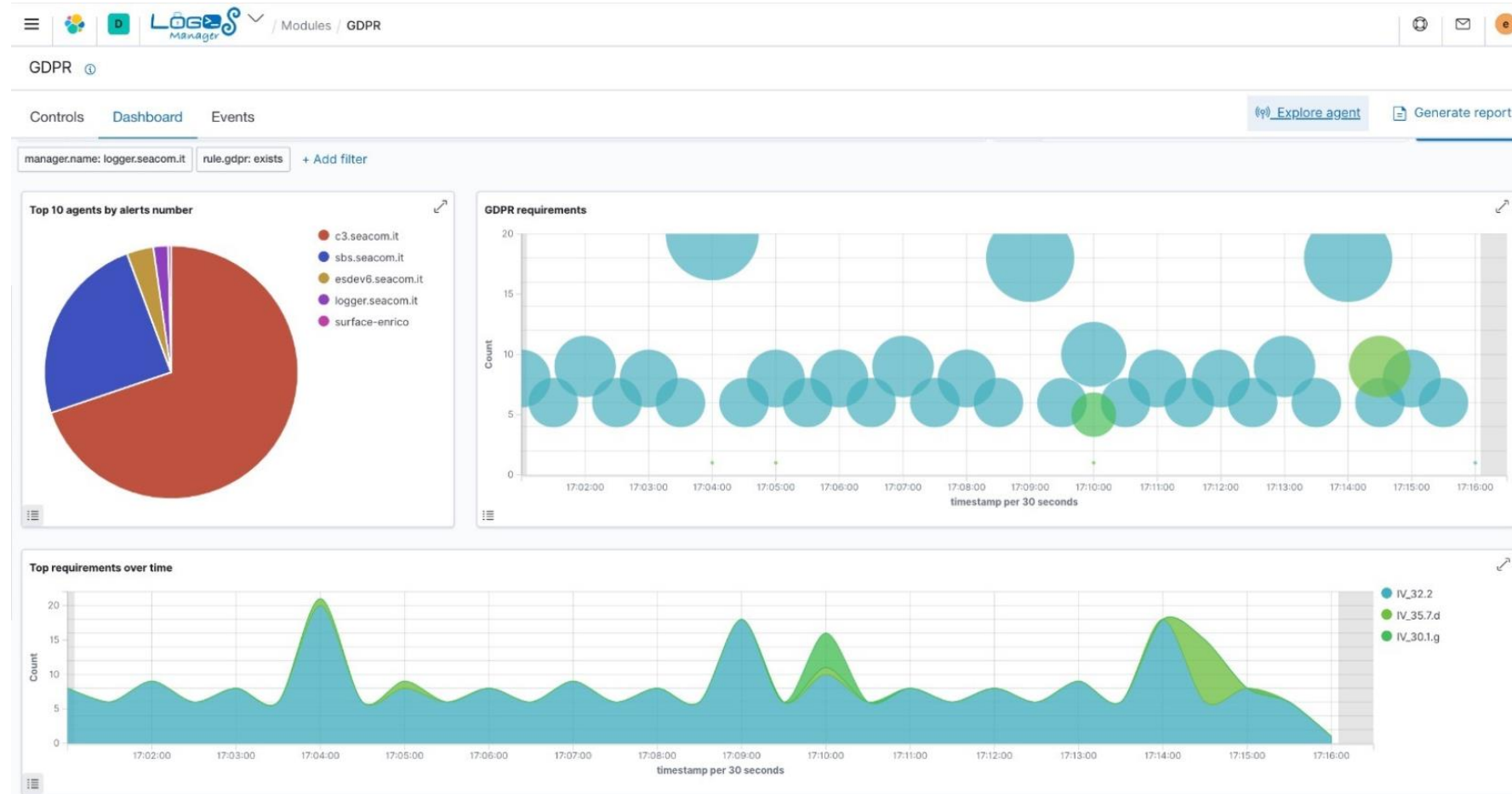
Log Data Analysis - Lettura e analisi dei LOG del SO e delle applicazioni: analizzati e archiviate in base a regole che permettono di evidenziare errori, configurazioni errate, attività dannose, violazioni della privacy, ecc.

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



Dashboard di investigazione dei requisiti delle varie normative

LOGO S

Modules / GDPR

GDPR ⓘ

Controls

Dashboard

Events

Search

manager.name: obs.seacom.it rule.gdpr: exists + Add filter

GDPR

Requirement IV 1813184

Requirement II 2076

Requirement III 0

Requirements

Filter requirements

IV_32.2 - Account management tools ... 1427861

III_17 - Permanently erase personal informa... 0

IV_32.1.c - Data Loss Prevention (DLP) cap... 0

Requirement II_5.1.f

Details

Requirement description

Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, verifying its modifications, accesses, locations and guarantee the safety of them. File sharing protection and file sharing technologies that meet the requirements of data protection.

Recent events

2076 hits

Search

KQL

Last 30 days

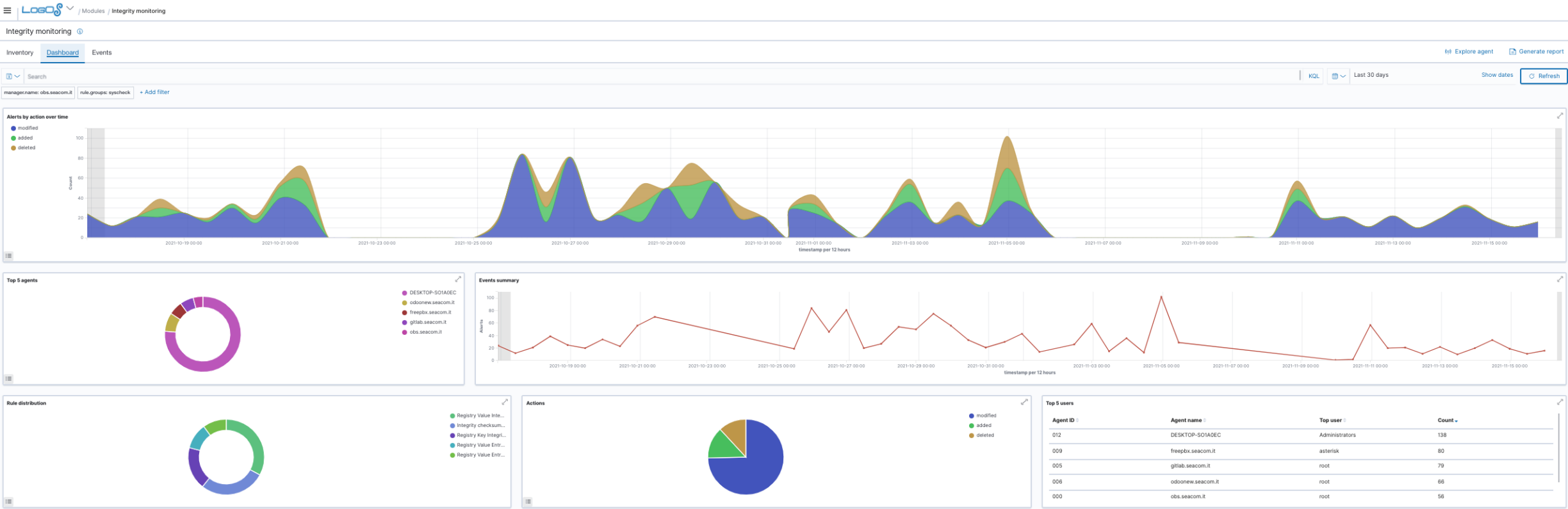
Show dates

Refresh

+ Add filter

Time ↓	Agent	Agent name	GDPR	Level	Rule ID	Description
> Nov 15, 2021 @ 10:04:36.367	003	mail.seacom.it	II_5.1.f	7	550	Integrity checksum changed.
> Nov 15, 2021 @ 09:06:17.812	009	freepbx.seacom.it	II_5.1.f	7	550	Integrity checksum changed.

Controllo costante dell’Integrità dei sistemi



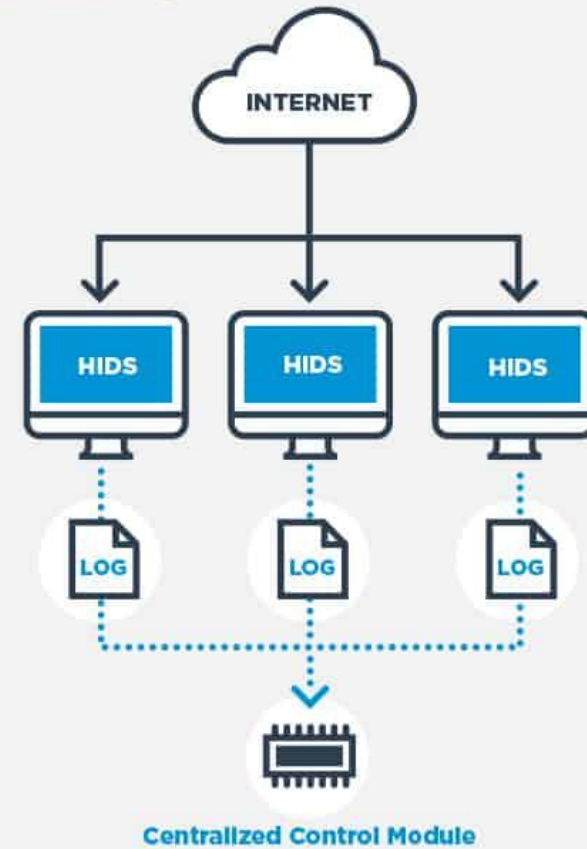
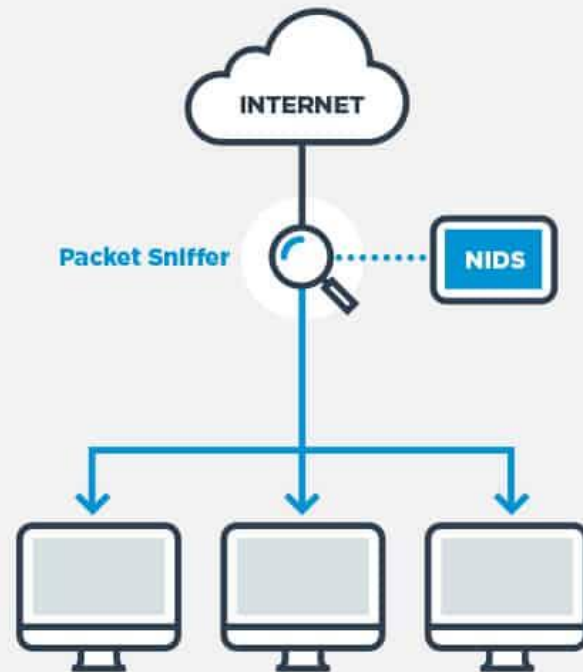


Security



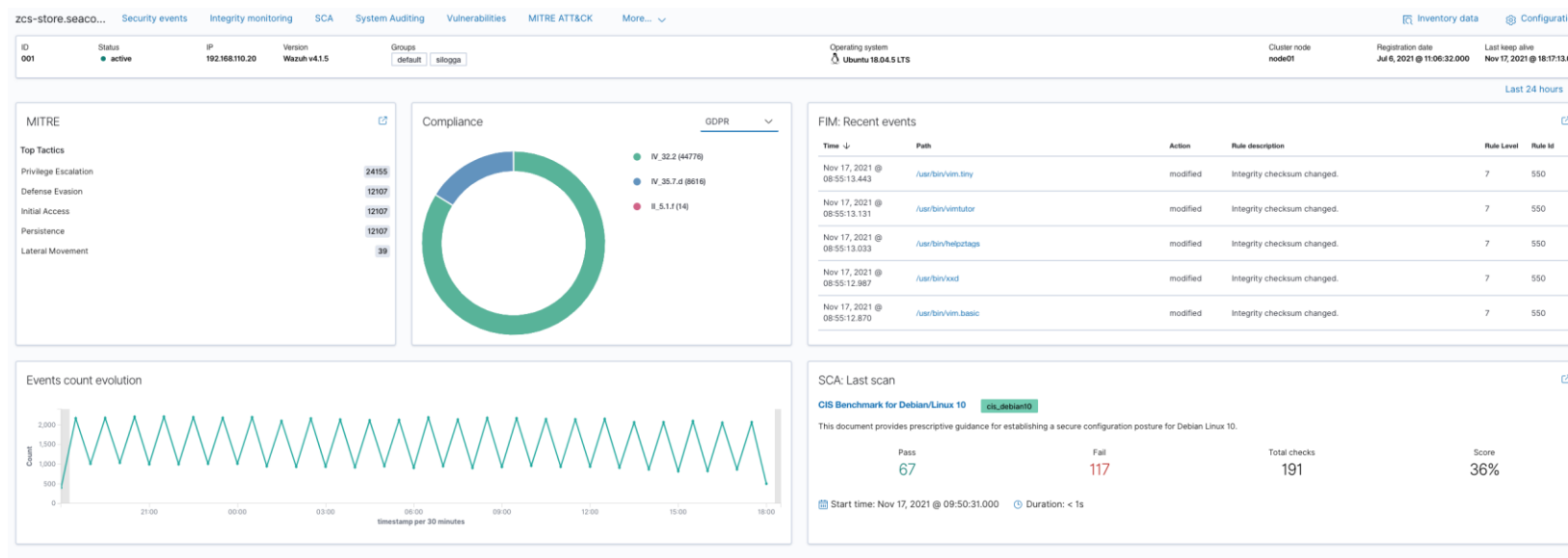
RETE ITALIANA
OPEN SOURCE

NIDS vs HIDS



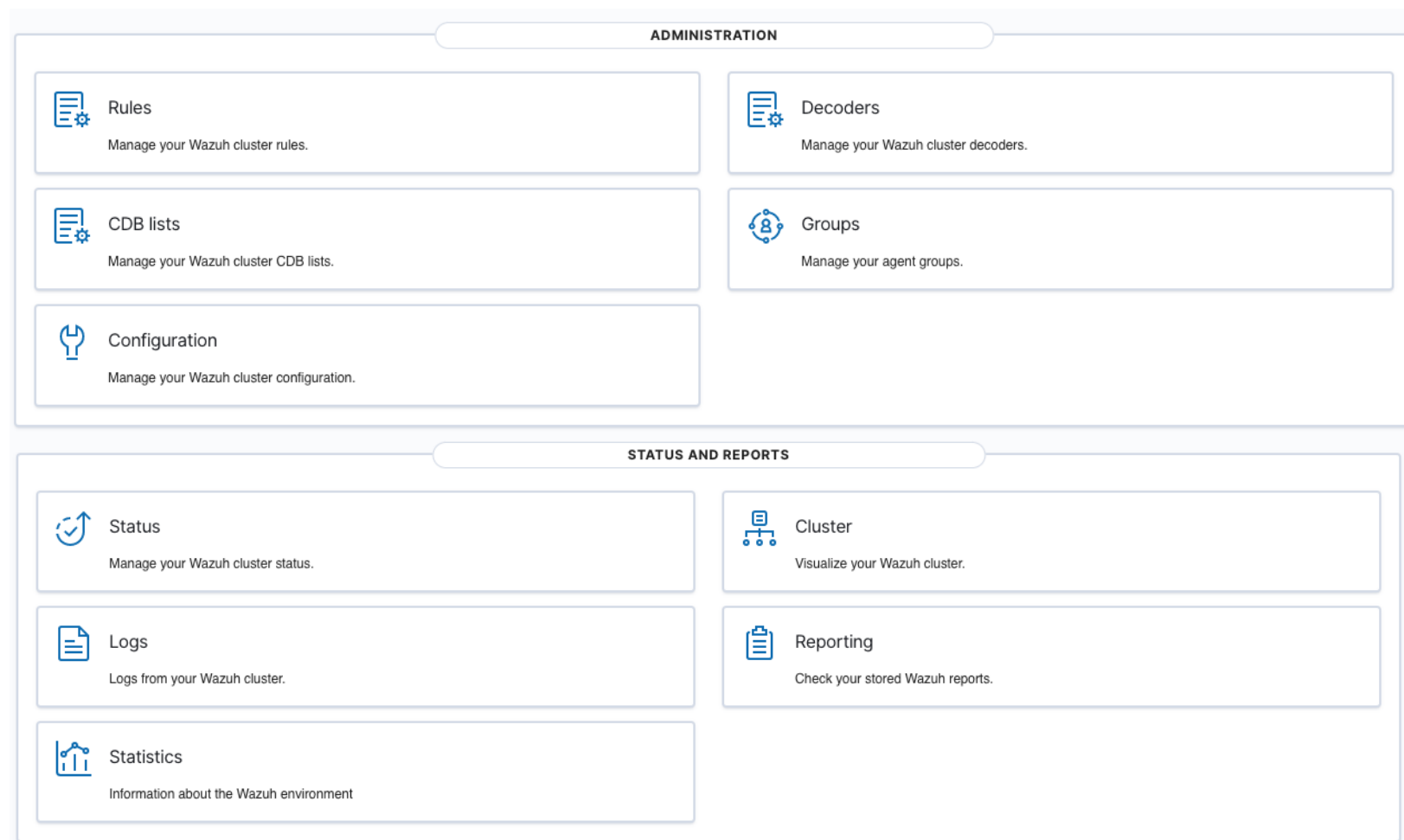
LE FUNZIONI SIEM

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



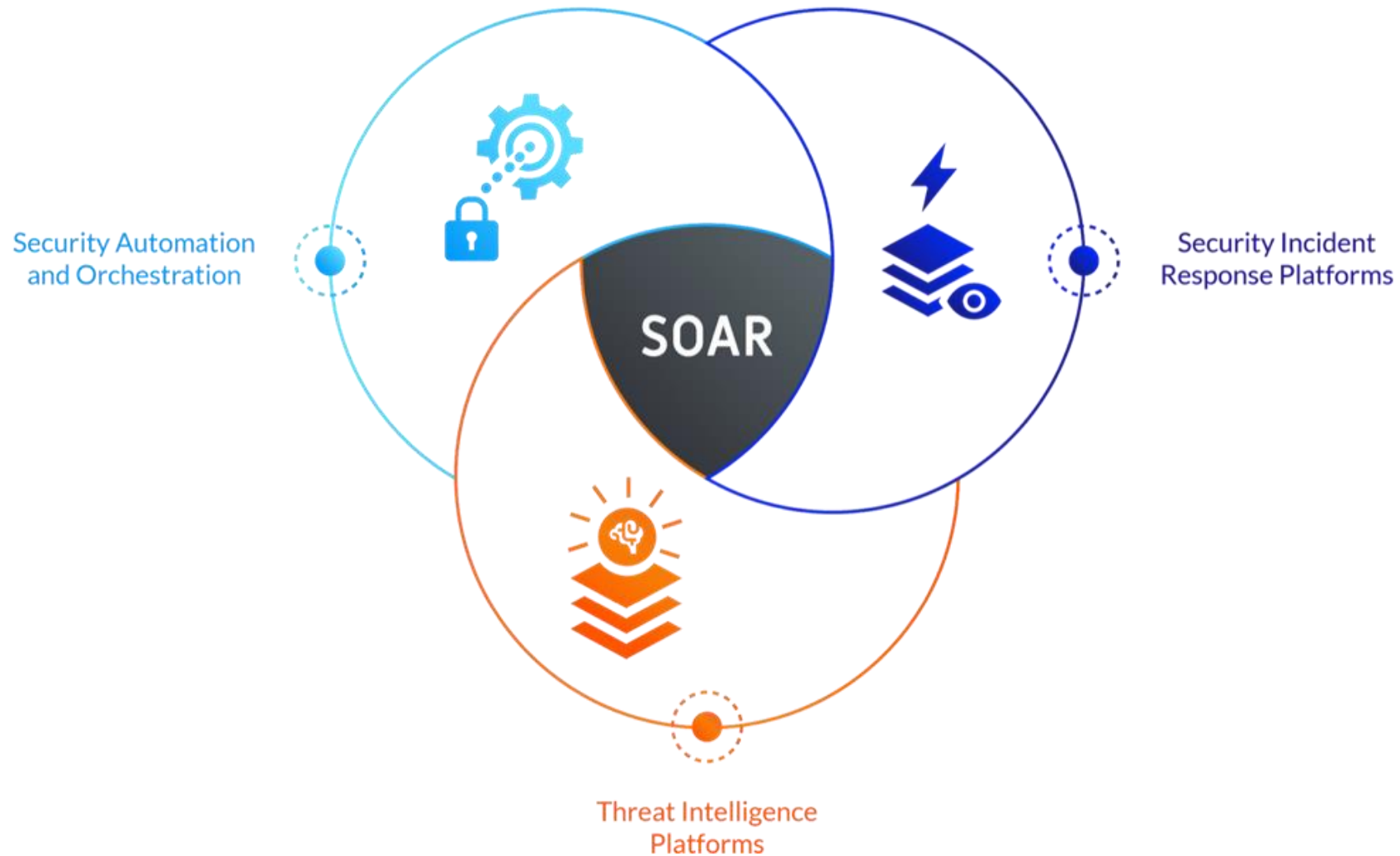
LA GESTIONE CENTRALIZZATA

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



LE INTEGRAZIONI

$$\text{SOAR} = \text{SAO} + \text{SIRP} + \text{TIP}$$



TIP – MITRE ATT&CK

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

MITRE ATT&CK ⓘ

Framework Dashboard Events

ⓘ Explore agent

Search

KQL



Last 30 days

Show dates

Refresh

manager.name: obs.seacom.it rule.mitre.id: exists + Add filter

Tactics



Privilege Escalation

711707

Defense Evasion

358396

Persistence

358229

Initial Access

358225

Credential Access

29928

Impact

1321

Lateral Movement

555

Discovery

1

Command and Control

0

Exfiltration

0

Techniques

Hide techniques with no alerts ☐

Filter techniques of selected tactic/s

T1078 - Valid Accounts

358223

T1169 - Sudo

353476

T1110 - Brute Force

29928

T1492 - Stored Data Manipulation

1149

T1021 - Remote Services

555

T1107 - File Deletion

172

T1485 - Data Destruction

172

T1050 - New Service

6

T1190 - Exploit Public-Facing Application

2

T1055 - Process Injection

1

T1083 - File and Directory Discovery

1

T1068 - Exploitation for Privilege Escalation

1

T1001 - Data Obfuscation

0

T1008 - Fallback Channels

0

T1024 - Custom Cryptographic Protocol

0

T1026 - Multiband Communication

0

T1032 - Standard Cryptographic Protocol

0

T1043 - Commonly Used Port

0

T1065 - Uncommonly Used Port

0

T1071 - Standard Application Layer Protocol

0

T1079 - Multilayer Encryption

0

T1090 - Connection Proxy

0

T1092 - Communication Through Removable ...

0

T1094 - Custom Command and Control Protocol

0

T1095 - Standard Non-Application Layer Proto...

0

T1102 - Web Service

0

T1104 - Multi-Stage Channels

0

T1105 - Remote File Copy

0

T1132 - Data Encoding

0

T1172 - Domain Fronting

0

T1188 - Multi-hop Proxy

0

T1205 - Port Knocking

0

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://panwdb1.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

The screenshot displays the TheHive web interface. The top navigation bar includes 'TheHive' logo, '+ New Case', 'My tasks' (1), 'Waiting tasks' (30), 'Alerts' (191), and 'Statistics'. A search bar on the right allows filtering by 'Case, user, URL, hash, IP, domain ...'. The main content area shows a 'List of cases (11 of 26)' with a table of incident details. The table columns are Title, Severity, Tasks, Observables, Assignee, and Date. The sidebar on the right provides a summary of alerts, including 'Closed by Bastard Operator', 'This is a new case', and 'Alert updates'.

Title	Severity	Tasks	Observables	Assignee	Date
#19 - [MISP] #3150 OSINT - Sofacy's 'Komplex' OS X Trojan by Palo Alto networks Tags: circ:incident-classification="malware" misp ioc src:CIRCL	H	5 Tasks	4		01/24/17 9:00
#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement Tags: Type:OSINT misp ioc src:CIRCL	M	5 Tasks	53		02/09/17 12:03
#21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook Tags: osint:source-type="blog-post" misp ioc src:CIRCL	L	5 Tasks	5		01/24/17 11:37
#20 - [MISP] #3107 OSINT - Turbo Twist: Two 64-bit Derusbi Strains Converge Tags: Type:OSINT misp ioc src:CIRCL	L	5 Tasks	10		01/24/17 9:04
#17 - #3024 OSINT - In the Shadows: Vawtrak Aims to Get Stealthier by adding New Data Cloaking Tags: Type:OSINT src:CIRCL	L	No Tasks	20		01/22/17 12:17
#15 - #13:#3395 Malspam 2016-09-22 (.js in .zip) - campaign: "Delivery #D-{integer}" / #14:Suspicious URL Tags: circ:incident-classification="malware" src:CIRCL suspicious url user report Merged from Case #13 and Case #14	M	No Tasks	16		12/13/16 13:17
#12 - #11:[Malspam] 2016-09-15 -- "SCAN" Campaign ? / #10:#3410 Malspam 2016-09-15 (.wsf in .zip) - campaign: "SCAN" Tags: malspam user report circ:incident-classification="malware" src:CIRCL Merged from Case #11 and Case #10	L	7 Tasks	12		12/13/16 10:24
#6 - #3211 OSINT - Malspam delivers NanoCore RAT Tags: ms-caro-malware:malware-type="RemoteAccess" enisa:nefarious-activity-abuse="remote-access-tool" osint:source-type="blog-post" src:CIRCL	L	No Tasks	1		12/07/16 22:23
#4 - #3414 OSINT OSX/Pintized Backdoor Additional Details by Zatz / Eric Romang Tags: Type:OSINT src:ChulhuSPRL.be	M	No Tasks	2		12/07/16 22:20
#3 - #3413 Malspam (2016-04-28) - Locky (#2) Tags: circ:incident-classification="malware" malware_classification:malware-category="Ransomware" src:CIRCL	L	No Tasks	19		12/07/16 22:18
#2 - #3407 NanoCore related activities	L	No Tasks	2		12/07/16 22:17

Alerts Summary:

- Closed by Bastard Operator (a few seconds)
- This is a new case** (1 task has been updated See all)
status: Resolved
resolutionStatus: Indeterminate
summary: blah
impactStatus: NotApplicable
- Closed by Bastard Operator (a few seconds)
- test case** (1 task has been updated See all)
status: Resolved
resolutionStatus: Indeterminate
summary: blah
impactStatus: NotApplicable
- Updated by Bastard Operator (7 minutes)
#4859
status: Ignored
- Updated by Bastard Operator (7 minutes)
#4858
status: Ignored
- Updated by Bastard Operator (7 minutes)
#4857 sakjdhsakjhdksahdsa
status: Ignored
- Updated by Bastard Operator (7 minutes)
#4860
status: Ignored
- Updated by System (35 minutes)
Alert updates
2 new alerts have been added
2 existing alerts have been added
See all
- Updated by System (38 minutes)
Alert updates
200 existing alerts have been added

SOAR – Shuffle

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



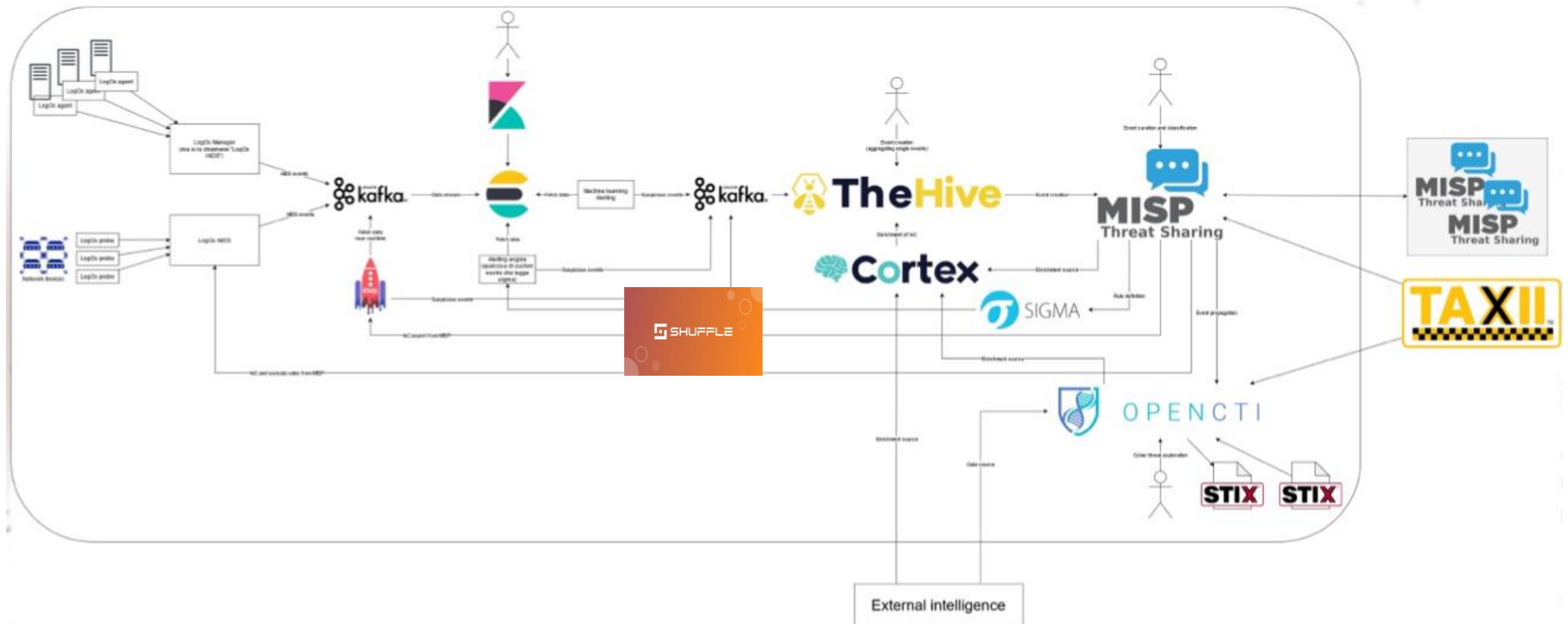


Stack Completo



RETE ITALIANA
OPEN SOURCE

HLD





#OSW2021



<http://www.reteitalianaopensource.net>



RETE ITALIANA
OPEN SOURCE