Borse di studio GARR
Orio Carlini

SISTEMA INTEGRATO DI SICUREZZA INFORMATICA PER LA GESTIONE PROATTIVA DELLE MINACCE

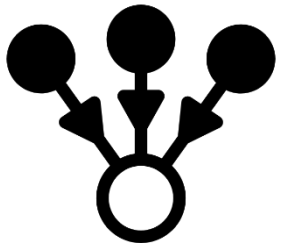
Nicolò Thei

Università degli Studi di Parma

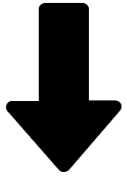
Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Contesto

Grandi quantità di Dati



Piattaforma Centralizzata

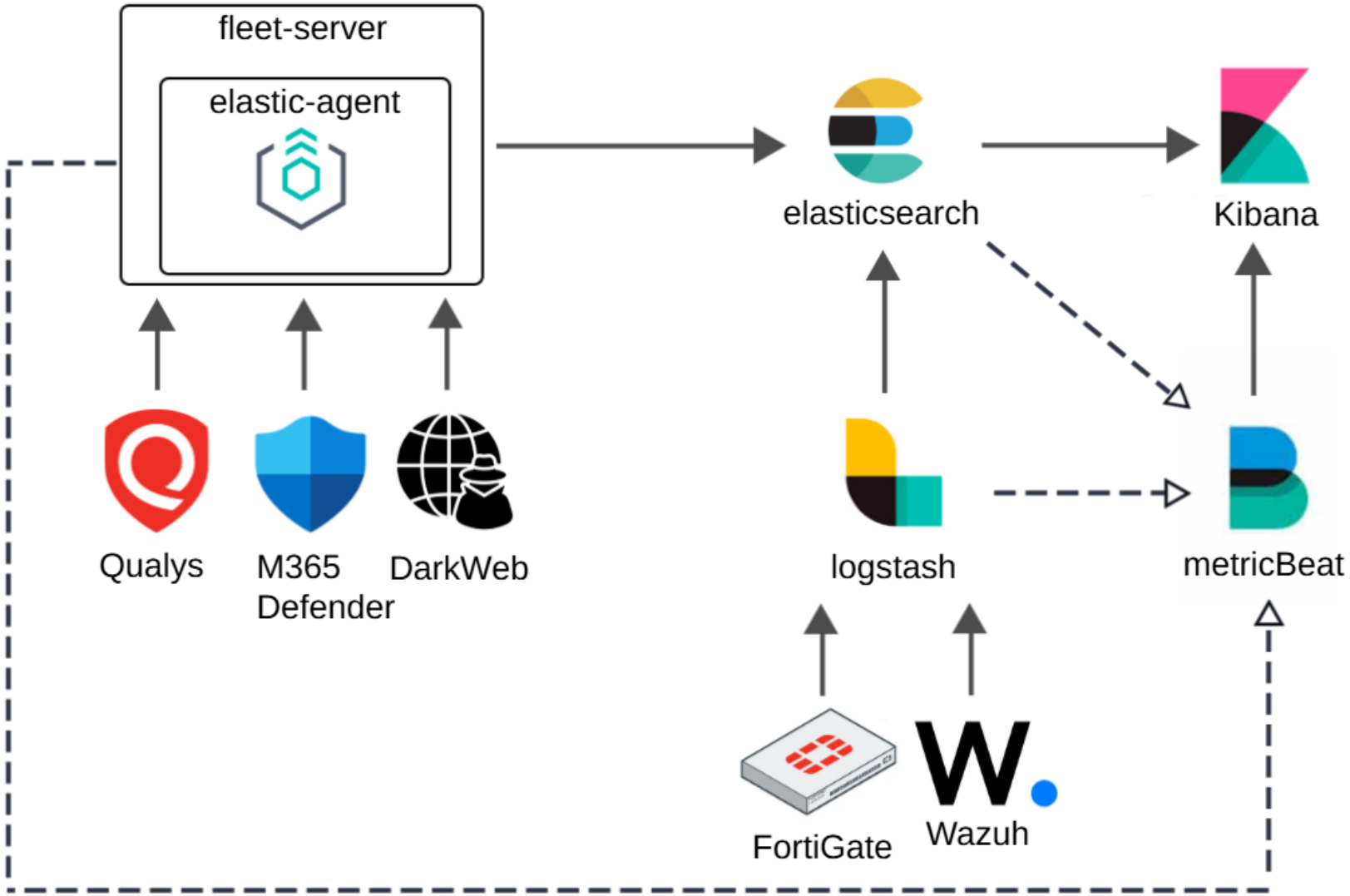


Individuazione dell’Attacco

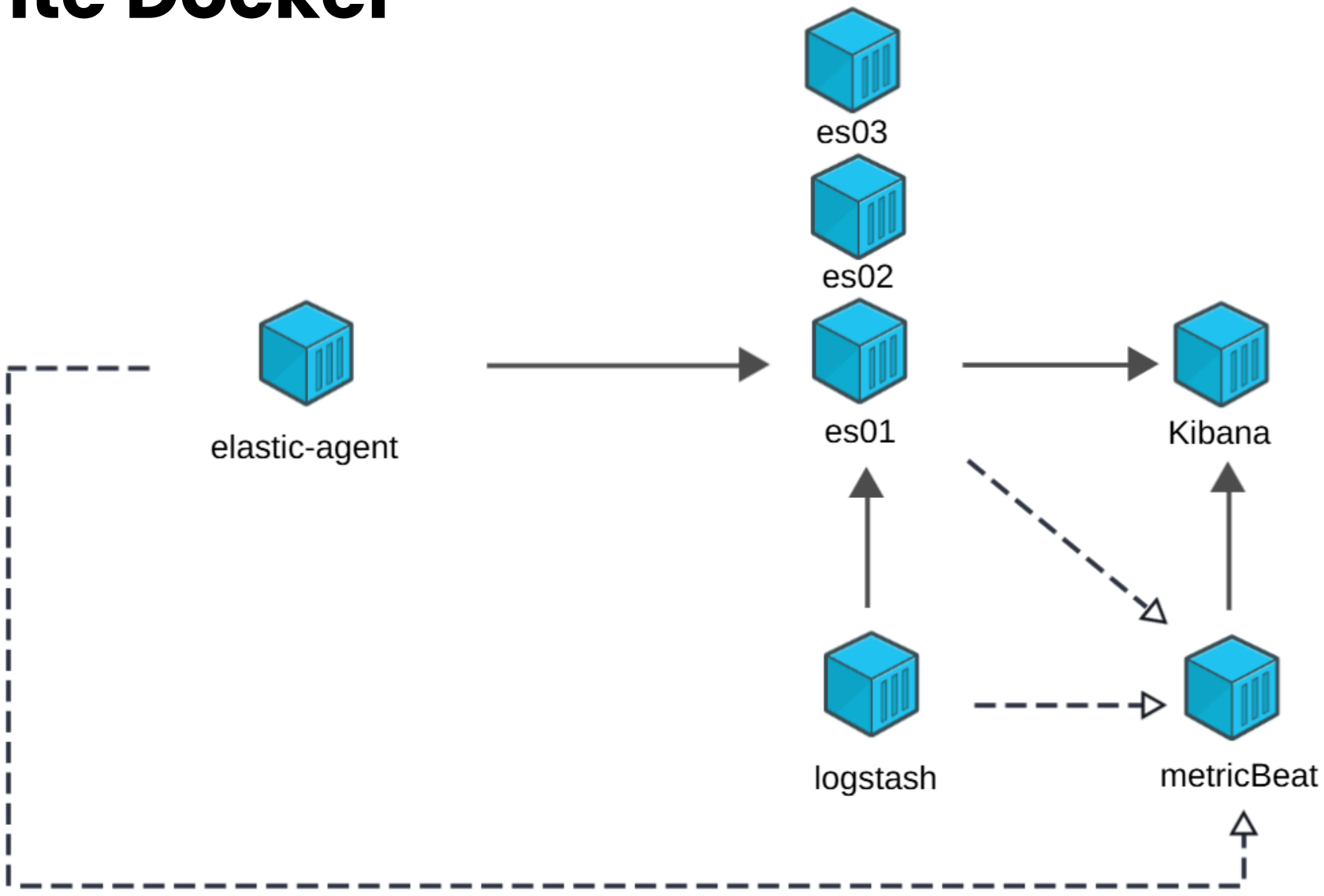
Obiettivi:

- Efficienza operativa
- Diminuzione tempo di risposta
- Conformità normativa
- Azioni correttive
- Rilevamento Anomalie

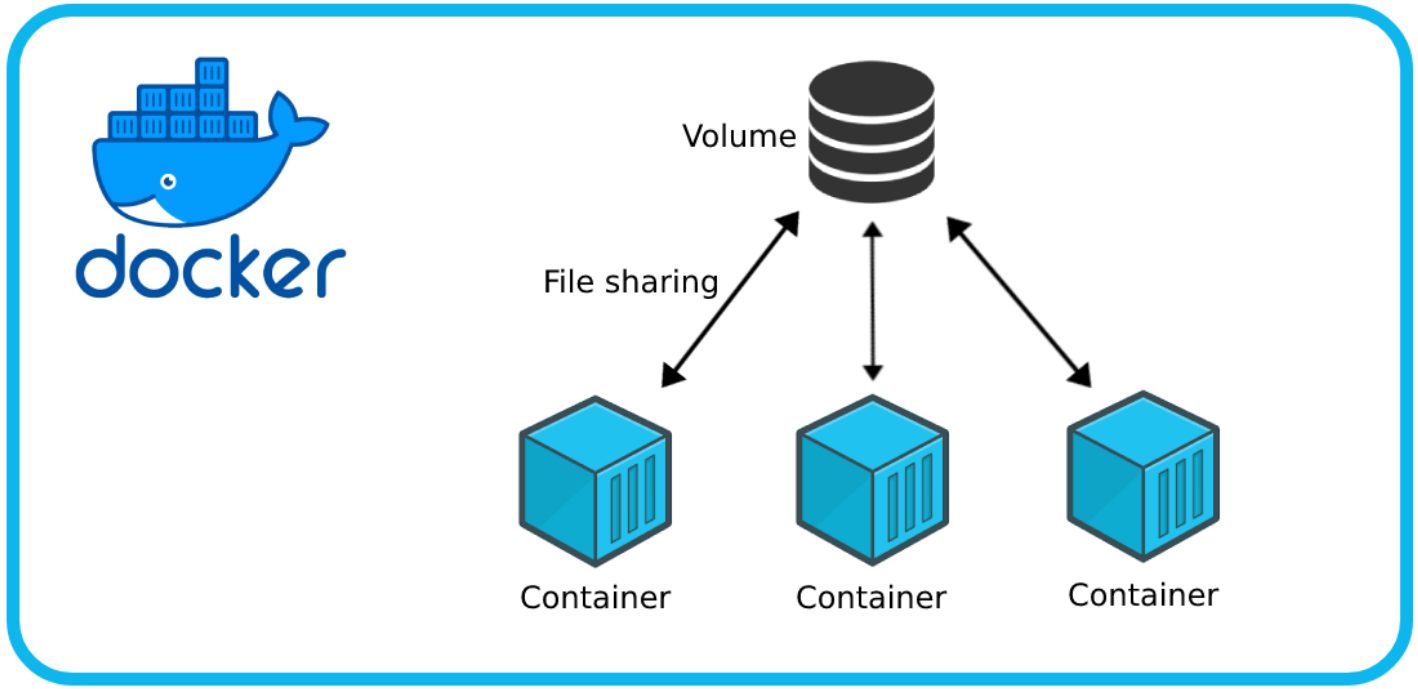
Ambiente Sviluppato



Ambiente Docker



Ambiente Docker

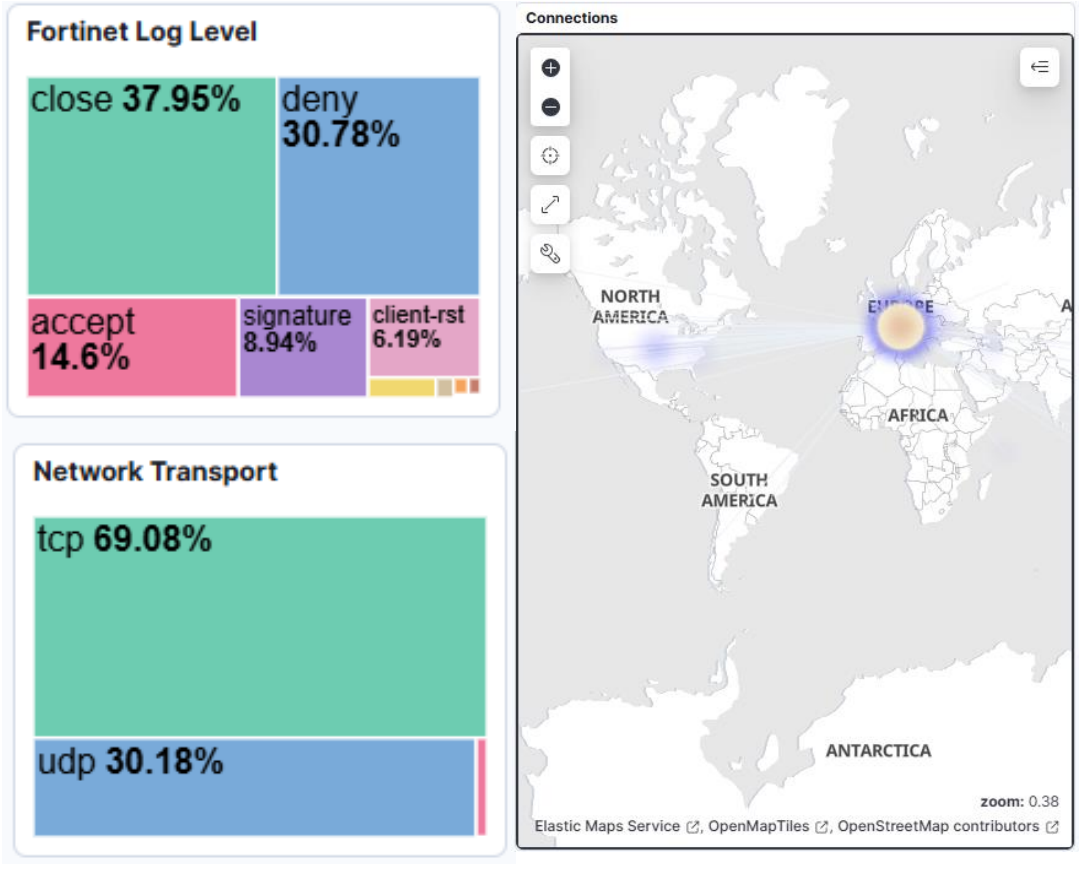


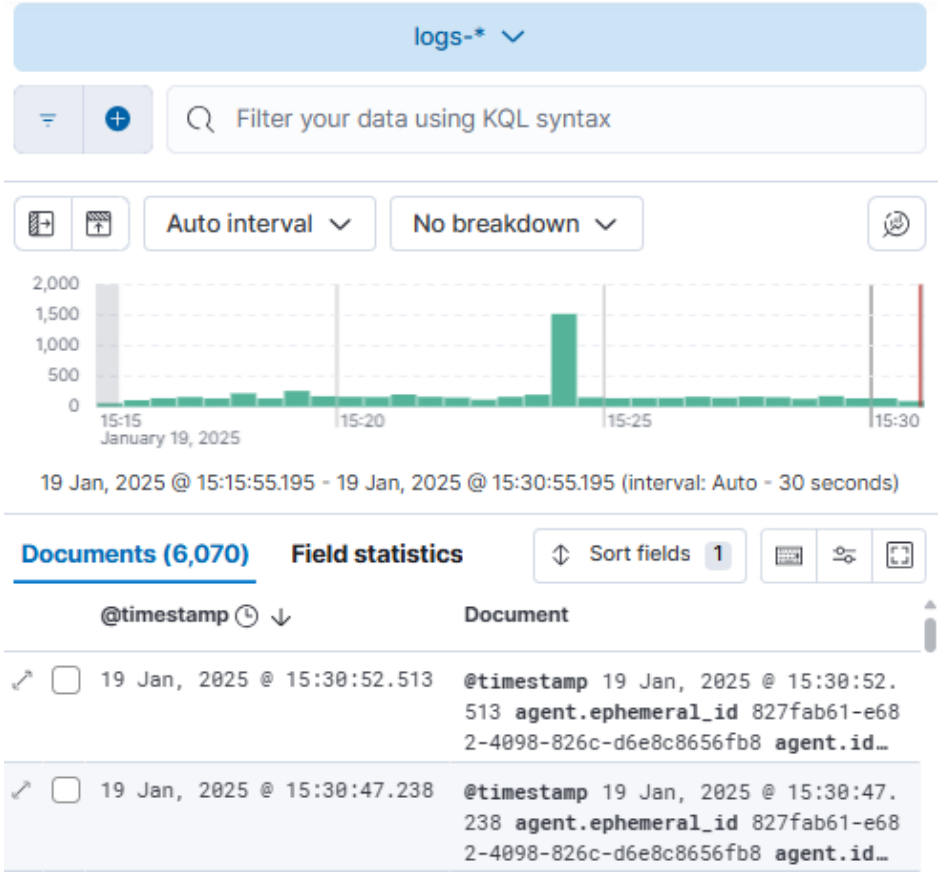
Specifiche Hardware:

3x16 GB RAM - Nodi ES

2 TB SSD *Binding Mount*

Visualizzazione Dati – Kibana UI





Caso di Studio

@timestamp	8 Aug, 2024 @ 16:08:23.216
m365_defender.alert.evidence.user_account.user_principal_name	[redacted]@unipr.it
m365_defender.alert.title	Unfamiliar sign-in properties
message	The following properties of this sign-in are unfamiliar for the given user: ASN, Browser, Device, IP, Location, EASId, TenantIPsubnet
related.hosts	sisa.priv
related.ip	91.236.[redacted]
threat.tactic.name	InitialAccess

SOAR

- Azioni di rimedio semi-automatizzate
  - Analisi Struttura **LDAP**
  - Web app **Django**

- Chiamata API:
  - Ripristino credenziali
  - Invalidazione Token
  - Invio E-mail di Recupero
  - Attivazione MFA

Rilevamento Anomalie

Time	Severity	Detector	Found for	Influenced by
September 20th 2024	87	Detects rare country names.	Brunei	destination.as.organization.name: Unified National Networks destination.geo.country_name: Brunei destination.ip: 202.160.xx.xxx

Sviluppi Futuri

- Adozione del **Machine Learning**:

  Algoritmi <u>non</u> Supervisionati
  - k-means clustering - Rilevamento Anomalie

  Algoritmi Supervisionati
  - Classificazione degli Alert (Critico, Moderato, Informazione)

- Analisi traffico tramite **TAP**

Borse di studio GARR
Orio Carlini

Grazie

Borsista: Nicolò Thei

Tutor: Raffaele Cicchese

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK