SCIOTEM
2024

BONDIOLI & PAVESI: SFIDA 1

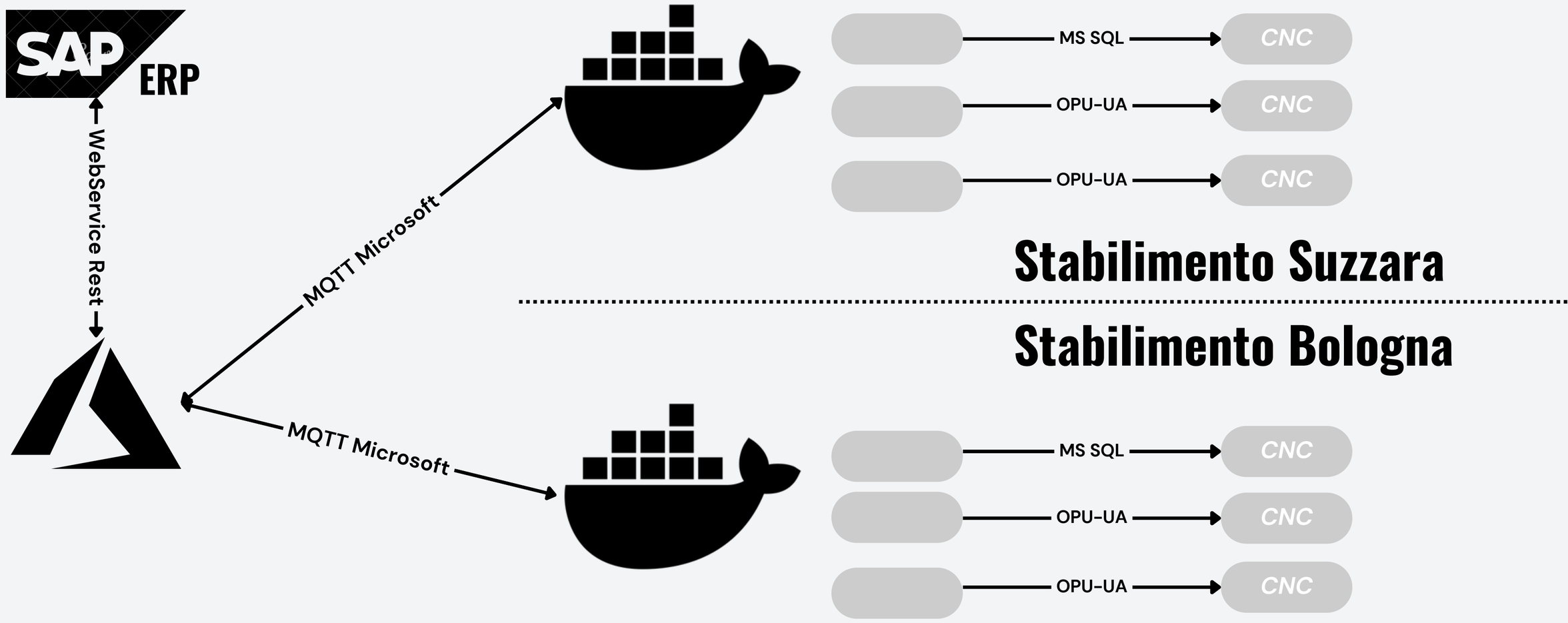
NFD

NETWORK FAILURE DETECTION

Leonardo Zini
Pietro Martinello
Gabriele Bassoli

CONTENT

STARTING POINT



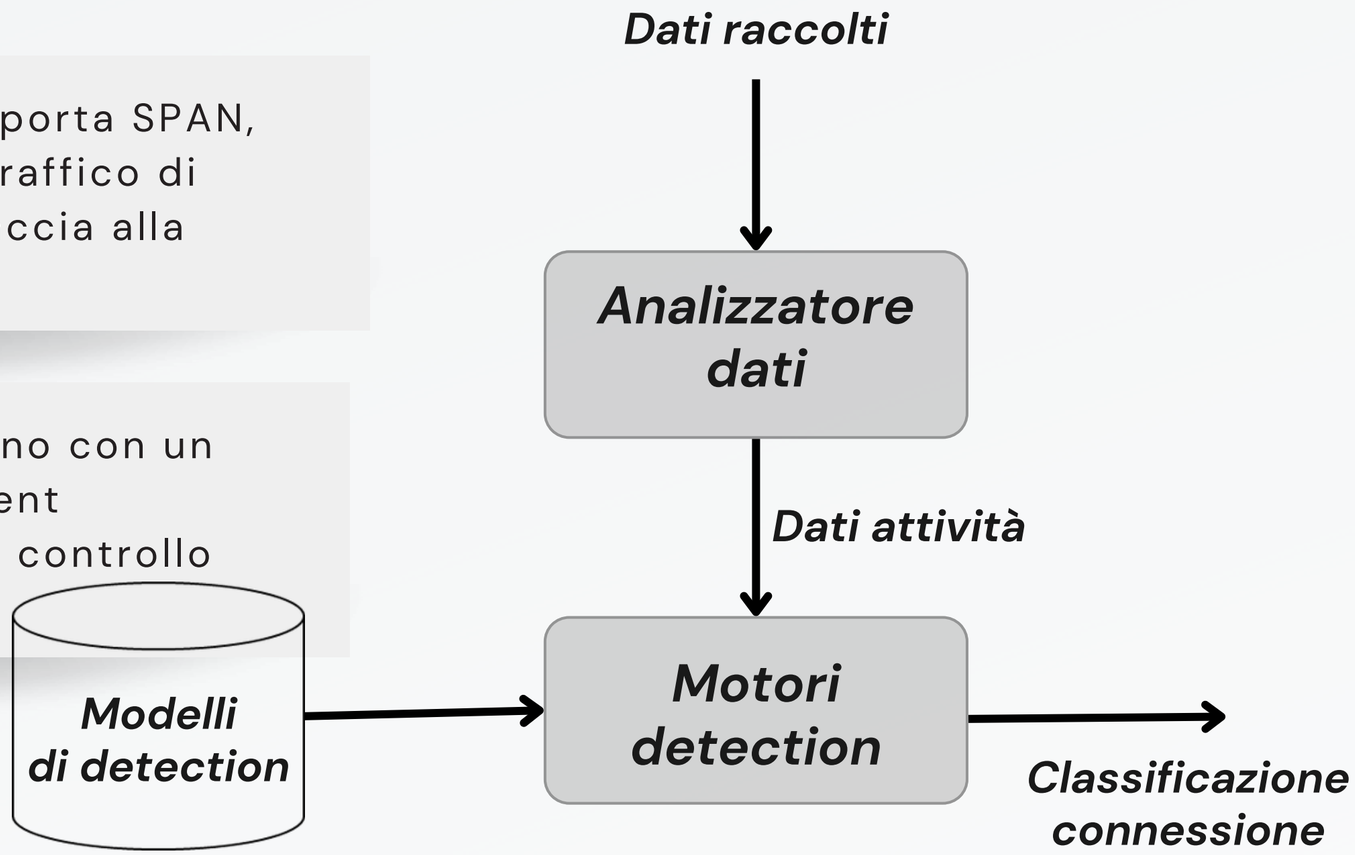
SOLUZIONE

La nostra interfaccia web per il monitoraggio controllato degli eventi.

IDS

Collegati ad uno switch sulla sua porta SPAN, un IDS è in grado di analizzare il traffico di rete con lo scopo di rilevare minaccia alla sicurezza.

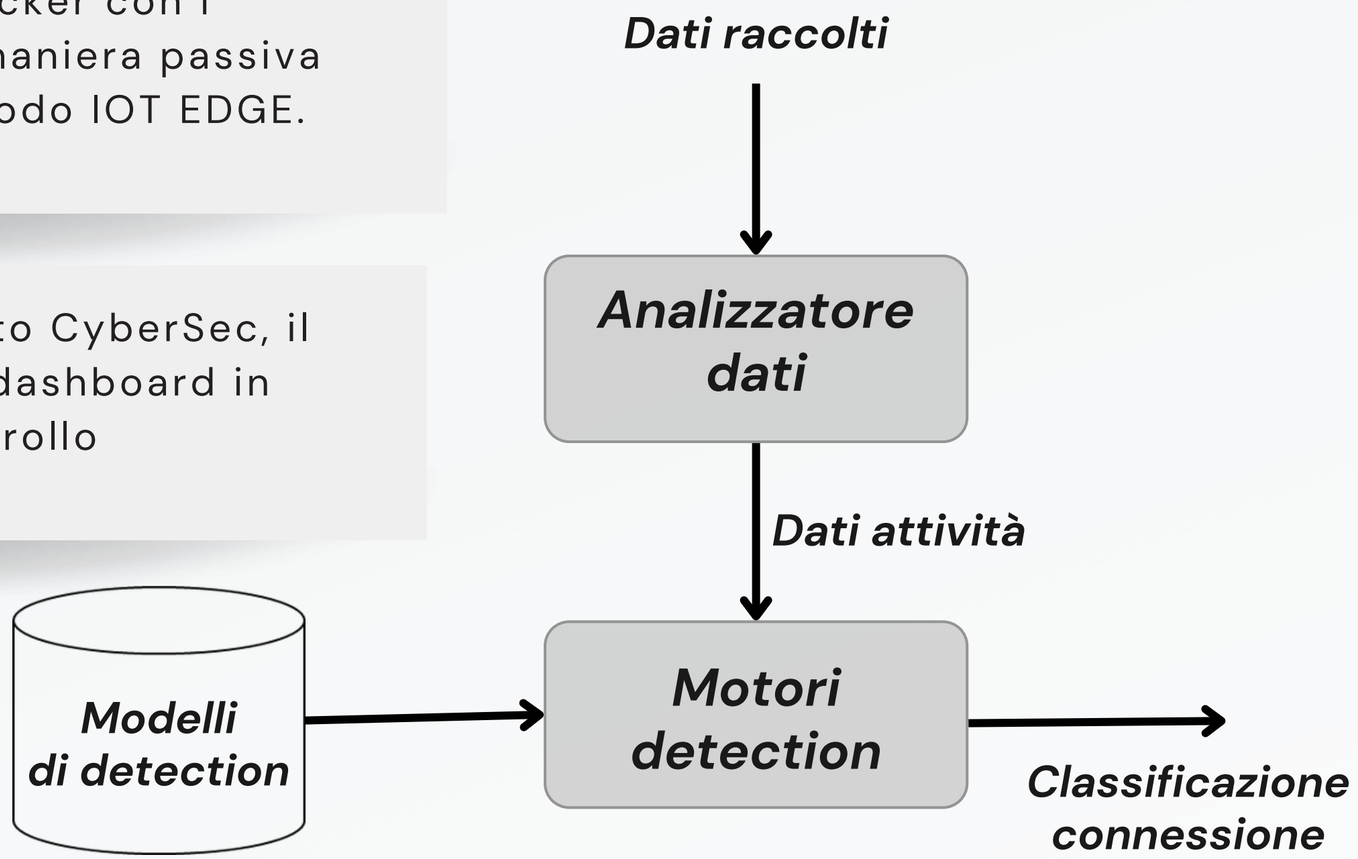
In CyberSecurity, gli IDS comunicano con un SIEM (Security Information and Event Management) in modo da avere un controllo centralizzato sui vari stati.



NFD

Software in esecuzione sul docker con i privilegi necessari, riceve in maniera passiva tutto il traffico in entrata al nodo IOT EDGE.

Parallelamente al SIEM in ambito CyberSec, il nostro NFD invia i dati ad una dashboard in cloud, in modo da avere il controllo centralizzato.



WHY?

Localizzazione

Un NFD è in grado di rilevare e localizzare non solo perdite di connessione ma anomalie delle connessioni, basate su pattern statici o attraverso motori decisionali basati sul **Machine Learning**.

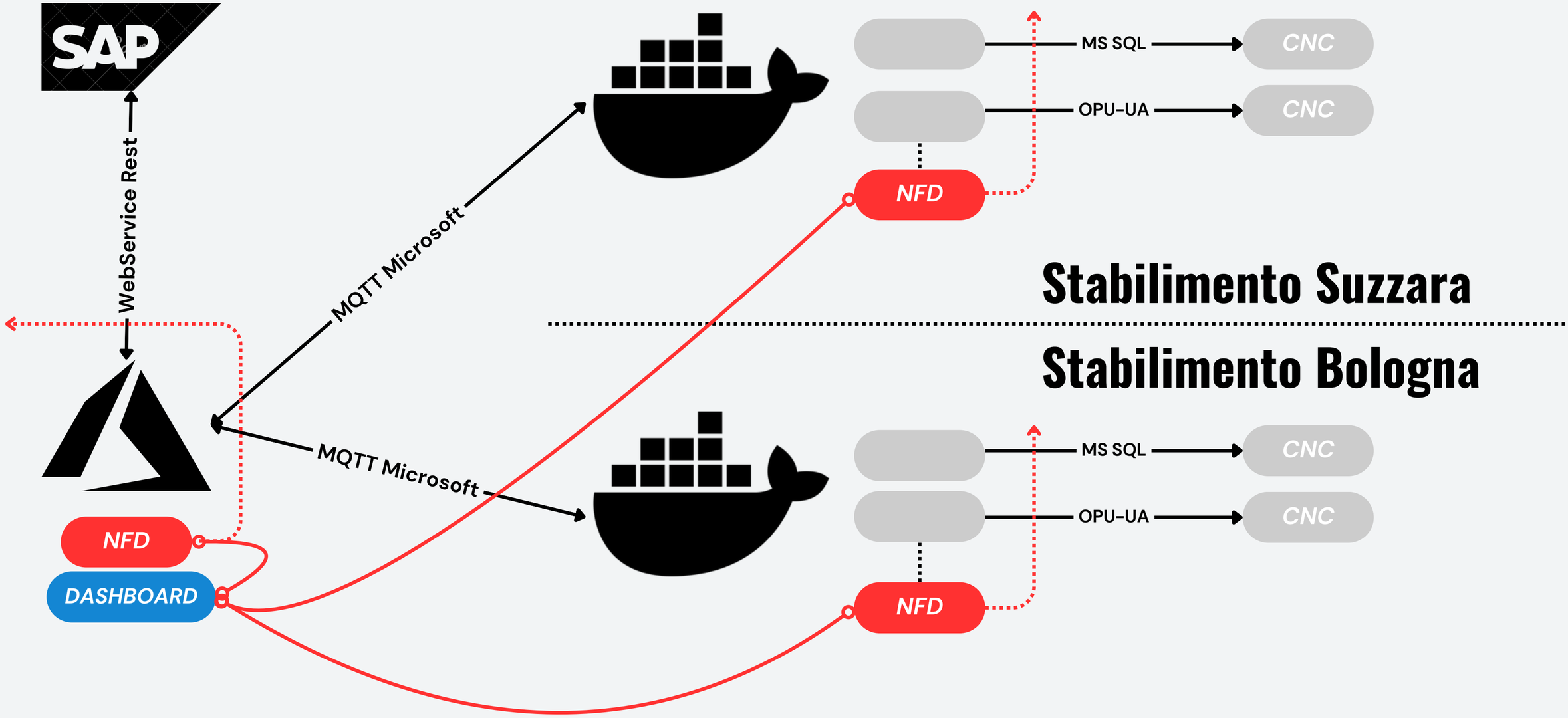
Basso impatto

Essendo un soluzione passiva, non agisce attivamente sulla rete, evitando di rallentarla ulteriormente nelle situazioni critiche.

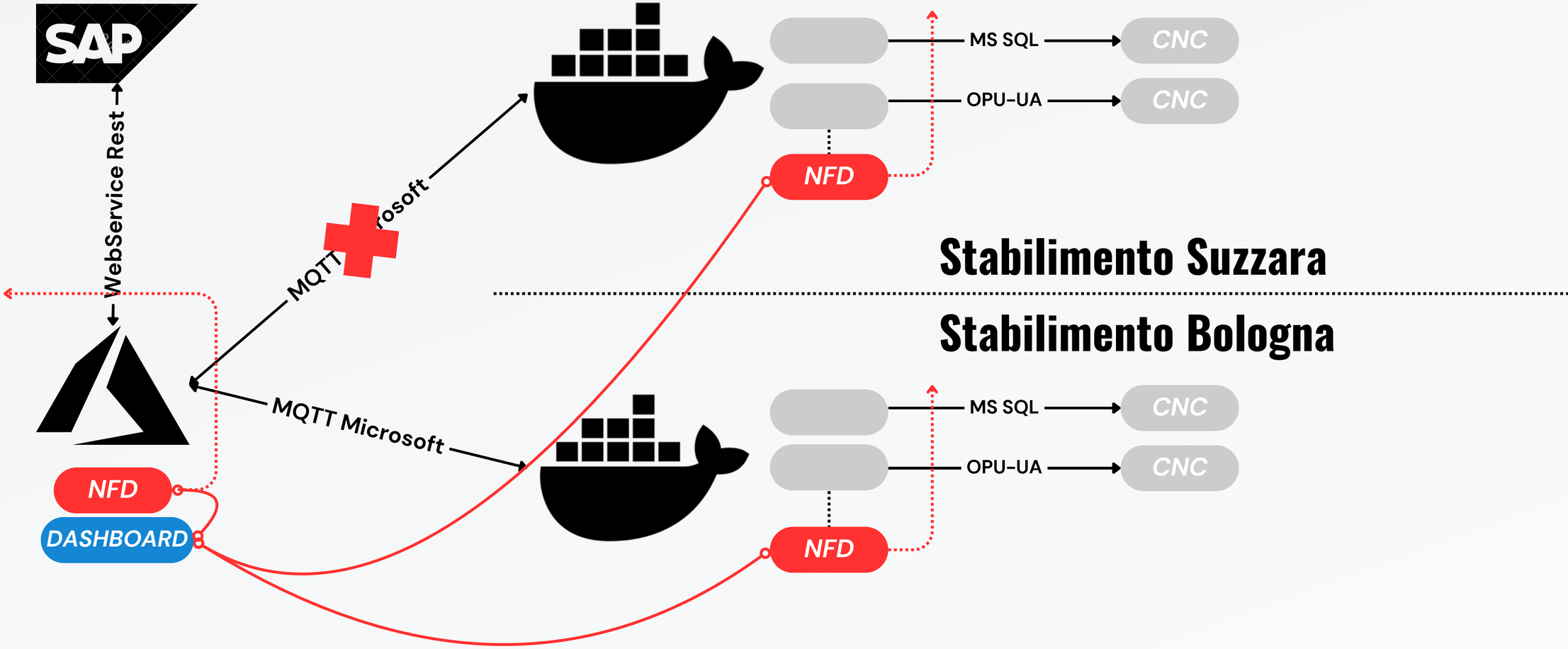
STRATEGY

Come tutto questo agisce nell’ecosistema presente.

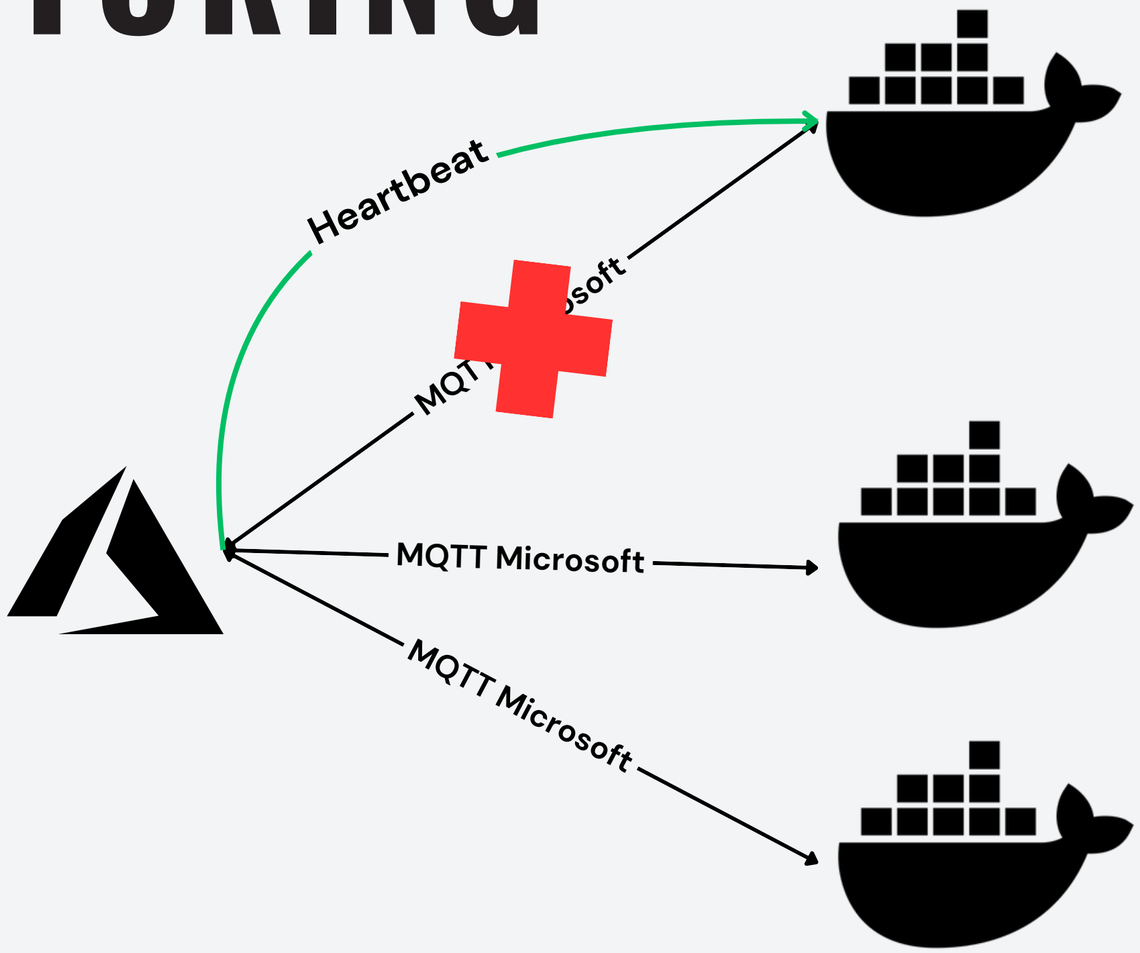
INFRASTRUCTURE



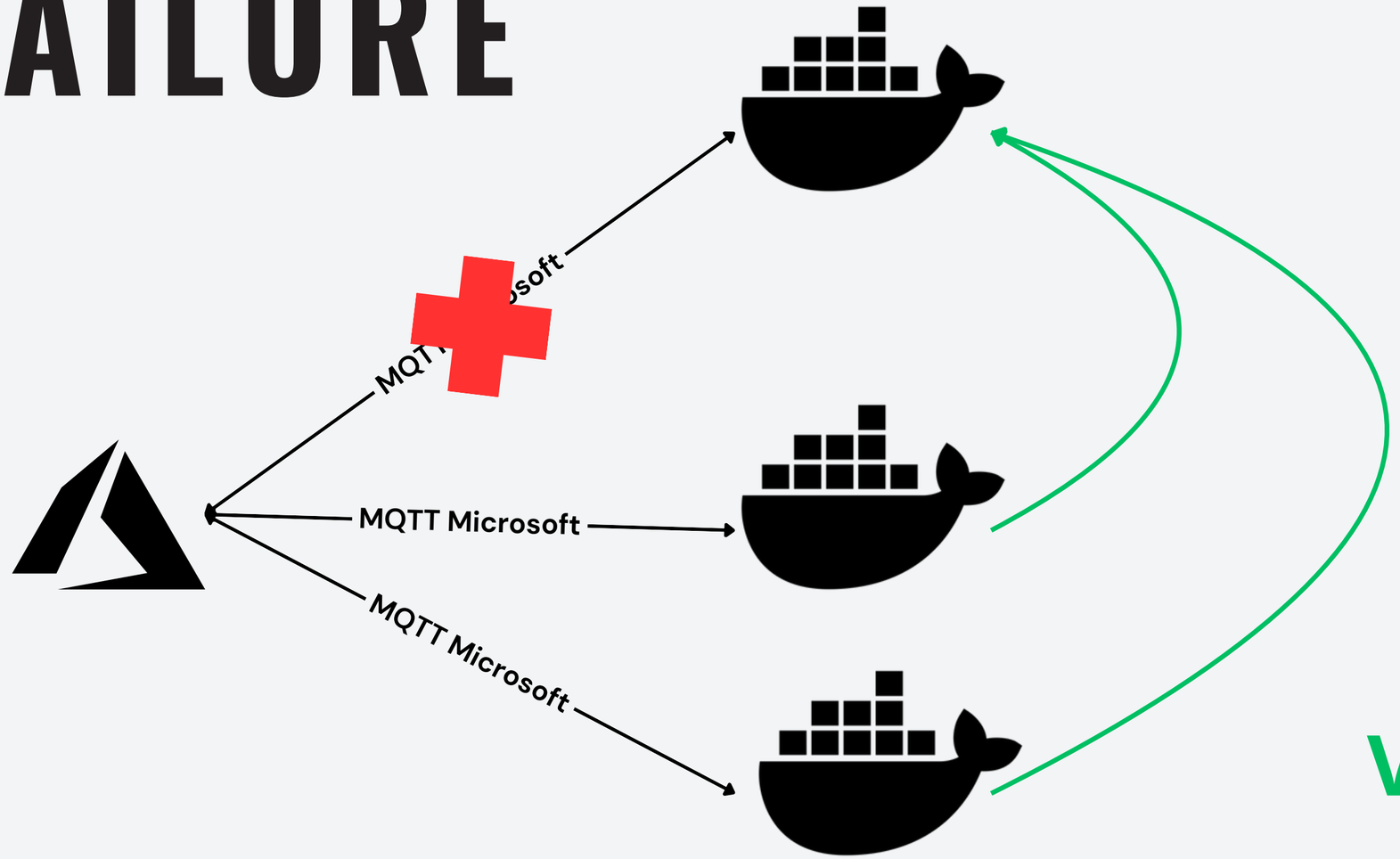
WHAT IF?


SAP
WebService Rest
MQTT Microsoft
MQTT Microsoft
NFD
DASHBOARD
MS SQL
CNC
OPU-UA
CNC
NFD
Stabilimento Suzzara
Stabilimento Bologna
MS SQL
CNC
OPU-UA
CNC
NFD

HEARTBEAT MONITORING



IOT EDGE FAILURE



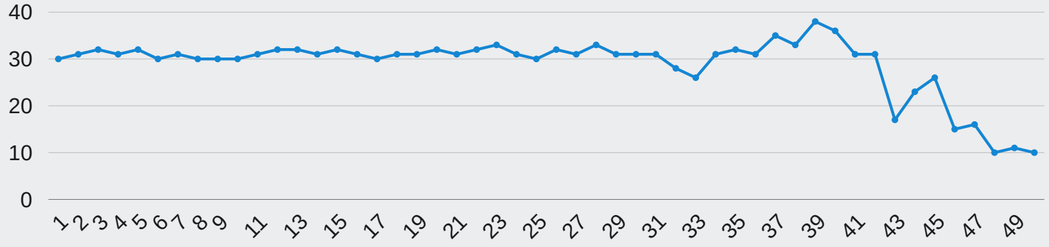
VPN STATE

DASHBOARD

La nostra interfaccia web per il monitoraggio controllato degli eventi.

CENTRO DI CONTROLLO

Network traffic

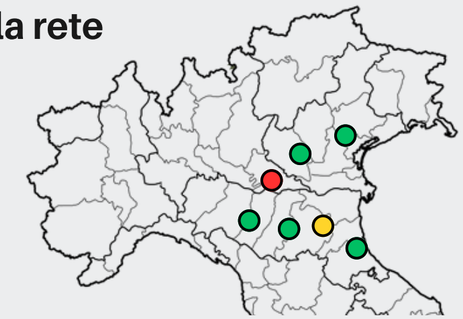


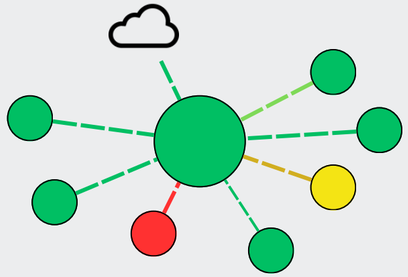
Status

Anomalie nella comunicazione con lo stabilimento di Suzzara

Dettagli

Overview della rete





Stabilimento: Suzzara

Dettagli

- CNC-A10B — Vedi Logs
- CNC-A23C — Vedi Logs
- CNC-B17N
- CNC-C17A
- CNC-A06E

Macchine attive **81%**

BONDIOLI & PAVESI

3 Notifiche non lette

NOTIFICATIONS

- Includiamo nel nostro sistema un meccanismo di notifica, in modo da notificare al dipartimento IT i problemi che si verificheranno.

- Il sistema di notifica è un bot di telegram, a cui ogni utente autorizzato può specificare il livello di verbosità delle notifiche.

TELEGRAM BOT

CONCLUSION

Con l’introduzione dei NFD e con un sistema di controllo degli stati distribuito, siamo in grada di localizzare errori e anomalie.

THANK'S FOR WATCHING

Leonardo Zini
Pietro Martinello
Gabriele Bassoli

SCIOTEM
2024