WORKSHOP GARR 2020

L'esperimento "Social" della Community: (il Bar del) GarrLab

Damiano Verzulli

damiano@verzulli.it

APM GARR
Università "G. d'Annunzio"
di Chieti-Pescara
http://www.unich.it

APM GARR
ICRANET Research Center
Pescara
http://www.icranet.org

“...da dove venite?”

- ...tutto parte dal “**grido di dolore**” lanciato al WS17...

GARR WorkShop 2017

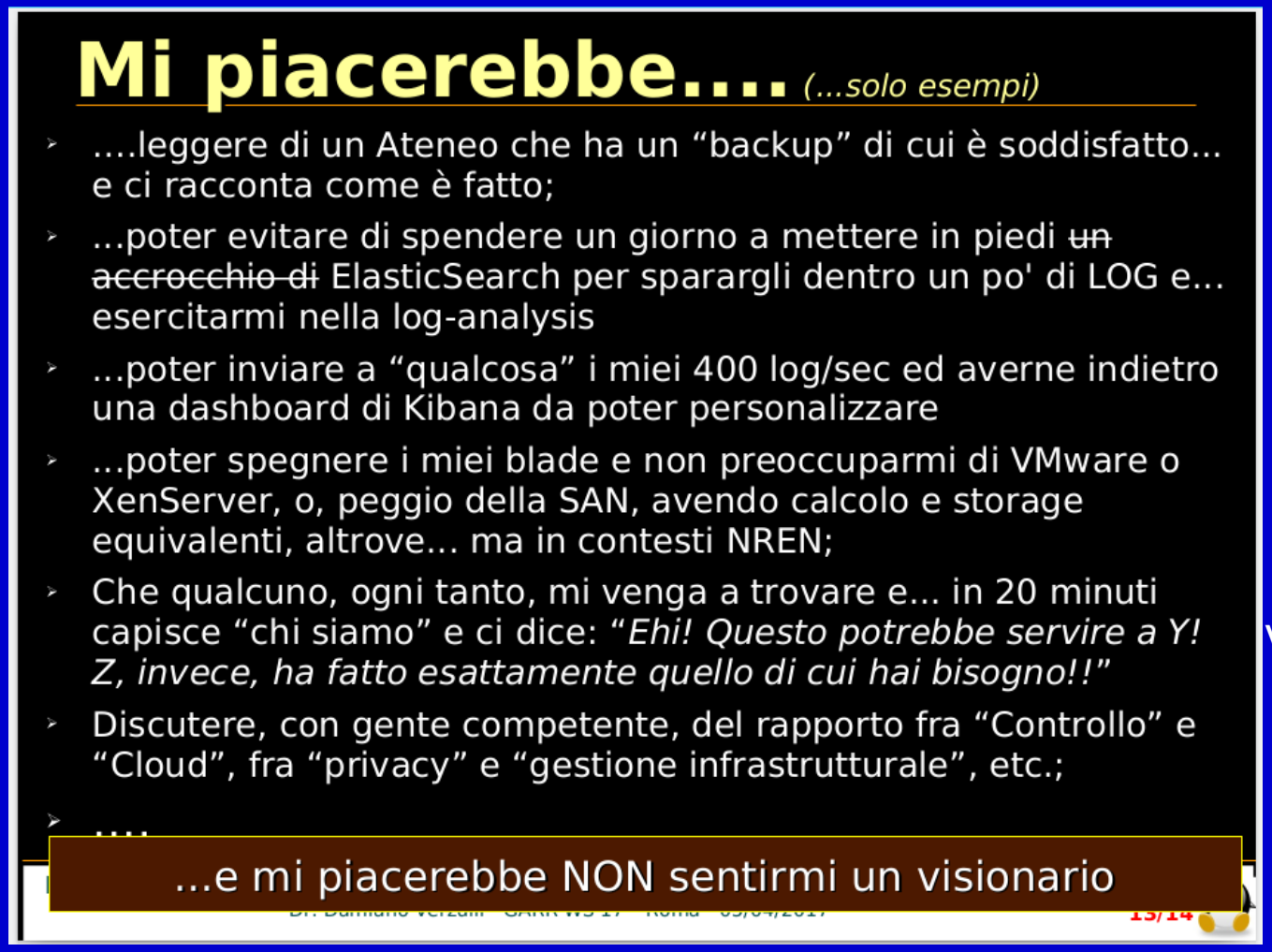
Intervento del 05/04/2017 dal titolo:

Il “futuro” (...ed il “presente”) visto da un (piccolo) ufficio “Reti e Sistemi”

Slide 9

“…da dove venite?”

- …e dal relativo “**desiderata**”



GARR WorkShop 2017

Intervento del 05/04/2017 dal titolo:

Il “futuro” (…ed il “presente”) visto da un (piccolo) ufficio “Reti e Sistemi”

Ultima slide

“...eravamo quattro amici al Bar...”

- Durante un coffee-break del **WS19**, scocca la scintilla: l’esigenza viene palesata anche da altri che condividono l’idea di “fare qualcosa”:
  - Giuseppe De Marco - UniCalabria
  - Francesco Izzi - CNR
  - Ermann Ripepi – CNR

- Due giorni più tardi, l’**11/10/2019**, nasce il gruppo Telegram dei

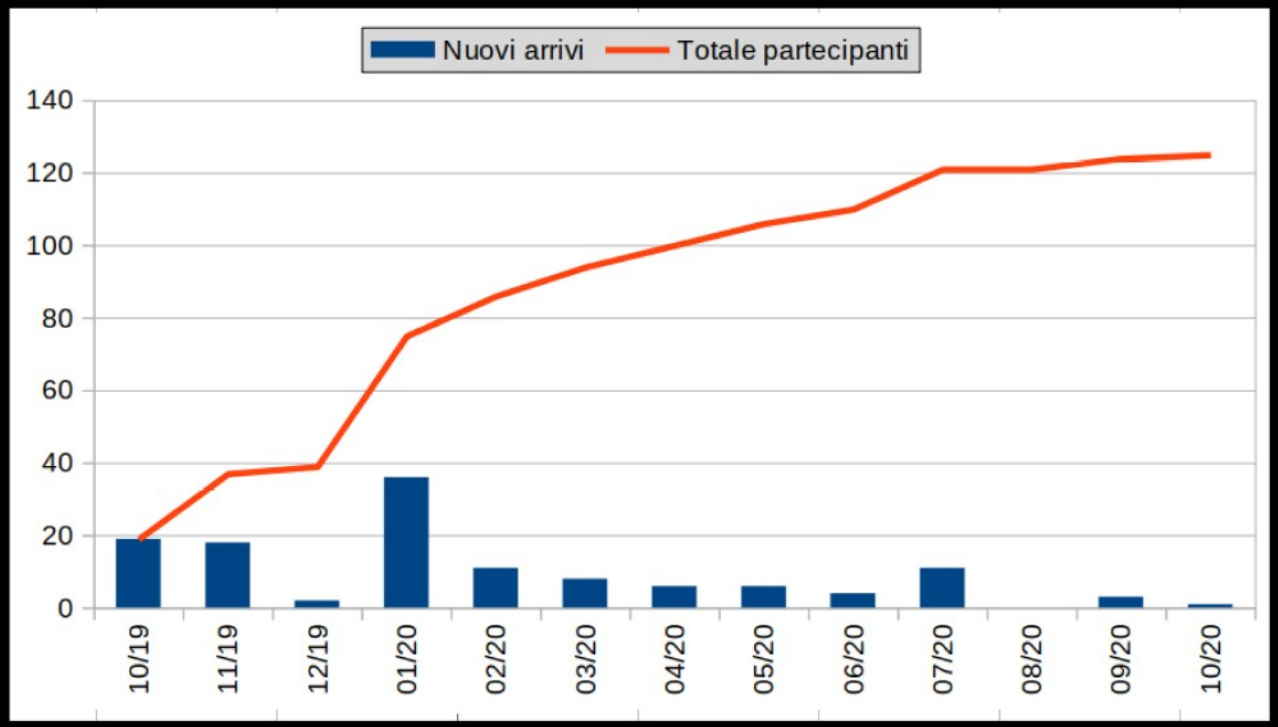
“**GARRisti Operativi (*al Bar*)**”

“Chi siete?”

- Con un moderato filtro all’ingresso ed una attenzione a non trasformarlo nel luogo di incontro degli alcolisti anonimi, il Bar è andato via via crescendo (come frequentatori e come volume di discussioni)

- Una costante è stata (ed è) quella di non snaturarne l’origine: **il Bar è dei “GARRISTI OPERATIVI”**, ossia di tutti coloro che vedono in GARR il “Grande Padre della Connettività” (*Principalmente Atenei, ma anche CNR, INFN, ed altri Enti [...oltre a GARR stesso ed a qualche “intruso”]*)

“Si, ma quanti siete?”



69 @ ~ 37 Atenei
19 @ Altri enti
28 @ GARR
3 @ (altro)

---

119 umani presenti
(+ 1 bot)

---

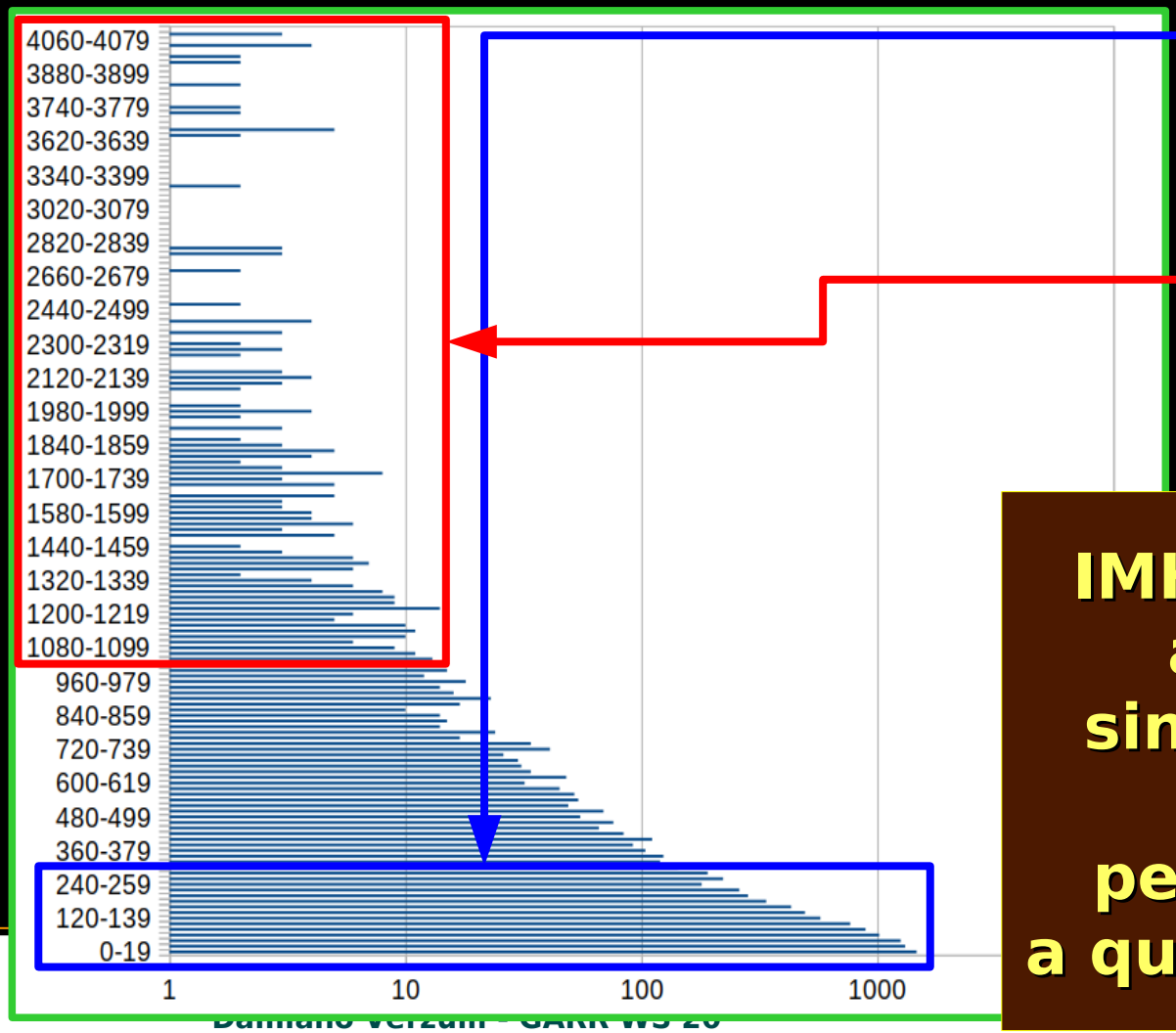
6 ci hanno salutato
(5 deleted account)

Pochi? Molti? ...Non so dirvelo :-(

Quello che so, però, è che il rapporto “segnale/rumore” è *MOLTO* elevato!

...e cosa dite?

- Distribuzione dei messaggi, per numero dei caratteri (SCALA **LOGARITMICA**!)

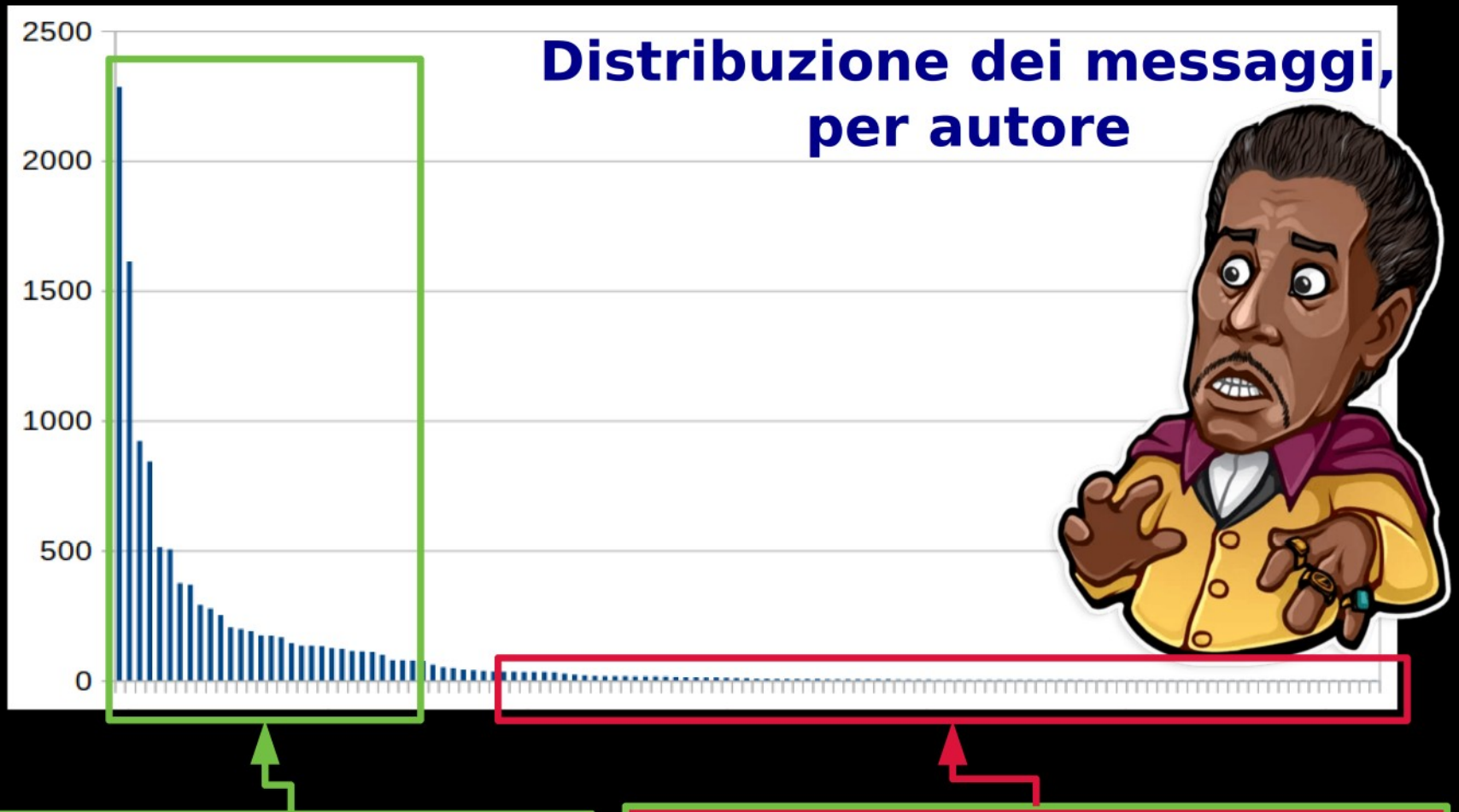


Molti messaggi sono particolarmente brevi (< ~250 char).

Ma i messaggi particolarmente densi di contenuto sono un numero rilevante!

IMHO, è sufficiente anche solo un singolo messaggio "giusto", per dare un senso a questo esperimento

Rose e fiori?



Il gruppo vive grazie al 20/30% degli iscritti

Più del 50% degli iscritti, di fatto, NON HA MAI POSTATO!

Qualche “Perla”!

- In un anno di attività, il Bar ha prodotto delle vere e proprie “perle” di conoscenza (ordine delle decine). Messaggi per i quali –IMHO– è valsa la pena di esserci… e (almeno) “leggere”

- Ne ho estratte **TRE**:
  - **Chiedo scusa in anticipo a tutti quelli che non citerò**: Non sarebbe possibile;
  - D’altronde ritengo necessario far capire cosa intendo per “perla”

Qualche “Perla”!

- Un paio di “trattati” sul SIEM
  di **Simone Bonetti** (CERT-UniBo)

“….Vi sento parlare di SIEM e da quel che recepisco ho la sensazione che non abbiate capito molto della cosa
[…]
- Non avete del tempo per addestrare un SIEM? Allora non avete bisogno di un SIEM…
- Wazuh è troppo difficile/ostico? Un SIEM commerciale non lo sarà di meno
- Wazuh non mi risolve il problema! => Un SIEM è un oggetto che segnala problemi. La reazione al problema va capita è ingegnerizzata.
[…]
il SIEM (open/closed non fa differenza) è una enorme lente d'ingrandimento: come ogni sistema di analisi vi fa vedere cose che voi umani non volete vedere :-D….”

Qualche “Perla”!

- Considerazioni “dal campo” sul complesso mondo del CLOUD

  di Federico Zani - INFN

“[Damiano] Lato GARRLab, ad esempio, un vincolo irrinunciabile era che "noi" (gestori) fossimo autonomi (sul firewalling) al 100%. Chiaramente questo ha un costo: non abbiamo utilizzato affatto i security groups di OpenStack e... abbiamo allestito due VM "dedicate" a questo scopo (una a PA, l'altra a CT). Il tutto era possibile grazie allo IAAS messoci a disposizione (OpenStack)

[Federico] **Qui secondo me vi siete tagliati da soli fuori dal bello di avere sistemi cloud sotto al sedere: senza funzionalità come i sec group, load balancer as a service, automazione, etc, OpenStack diventa un “semplice” sistema per fare spawn di vm.**
[*...e tutta un’altra lunga serie di considerazioni interessanti...*]

Qualche “Perla”!

- Router di backbone (GARR; 10G) implementato con una VM Linux

di Fabio Pedretti - UniBS

“ la VM "router" ha due interfacce: eth0 untagged su cui arriva solo il link GARR. Ed eth1 su cui ci stanno tutte le VLAN interne [...]
Routing: solo statico

Firewall: iptables + varie blacklist caricate con il tool di FireHOL (che usa ipset e ottimizza le regole consolidando le reti [...]

I server sono 3 Dell PowerEdge con 2 socket Xeon, complessivamente le CPU sono utilizzate circa al 25%.
La VM del firewall attualmente ha 6 core e sono usati durante il traffico di punta circa al 70%...”

Realizzato internamente a costo zero, ha consentito risparmi significativi in termini di TCO

...anche tanto vino buono!

Oltre alle “perle”, ci sono stati anche numerosi (~ cinquantina) spunti di discussione che non sarebbero esistiti…. senza il Bar. Qualche esempio:

- Troubleshooting di un problema con Facebook @ UniBS + UniCH + UniParthenope (192.167.0.0/20)
- Analisi e troubleshooting del DDOS/Reflection “Lottomatica” (con annesso SYN-Flood outbound)
- Spunti e discussioni su temi importanti (Privacy; Supporto alla Didattica; Aspetti normativi; Bandi/opportunità; lo stesso GARR ed il ruolo di APM)

Che tutto questo sia accaduto esclusivamente “pro-bono” lo considero un SUCCESSO!

Le “sale fumatori”

Qualche volta gli ospiti del Bar hanno chiesto le chiavi di una “sala fumatori”. Sulla porta c’era (c’è) scritto:

- ELK
- Infrastruttura AD
- Infrastruttura GarrCloud
- SIEM - Wazuh

- Altre volte gli stessi ospiti hanno scovato qualche altro piccolo bancone:
  - “GARRisti Tech…nicisti (al Bar)” (36 banconisti)
  - “GARRisti Makeristi” (12 banconisti)

Ho la sensazione (mia; personale) che il Bar sia diventato un posto dove, “finalmente”, si possono condividere “gioie e dolori” del proprio lavoro (…e del proprio DNA “tecnico”)

L’officina di fianco al Bar

Poco dopo l’apertura del Bar, abbiamo chiesto al…. proprietario dell’Immobile (ndr: GARR) di darci una “officina”, dove divertirci a fare “tuning” delle nostre auto.

Un ”GRAZIE, GARR” a nome di tutta la community: senza di voi, tutto questo NON sarebbe stato possibile.

*Un grazie “particolare” a **Massimo Carboni** (per il tempo e le risorse dedicate ai banconisti) ed a **Claudia Battista** (per la fiducia mostrata nei nostri confronti)*

L’officina di fianco al Bar

l’officina è un posto… strano:

- È ampia e ricca di strumenti al punto tale da rendere possibile… qualunque attività;
- È piena di carrelli con dentro attrezzi mai visti. Di alcuni si è sentito parlare; di altri si ignorava l’esistenza… e non si sa come utilizzarli;
- Alcuni attrezzi suscitano sensazioni di “amore/odio”: li vorresti prendere ed usare… ma sai che –quasi certamente– ti farai male.

L’intera sessione pomeridiana del WorkShop sarà dedicata all’officina!

L'officina... fa miracoli :-)

In officina ci sono diversi che lavorano (~ decina) e diversi che hanno dato un'occhiata (~ ventina).

Alcuni hanno creato dei veri e propri "tesori":

- Progetto "ecs-logstash"

  di Michele Albrigo - UniVerona

Fra APR e GIU 2020, Michele ha pubblicato – in "31 commit":
- il template degli indici di ElasticSearch utilizzati per la raccolta dei suoi LOG in formato ECS
- le sue 13 pipelines utilizzate per filtrare, analizzare ed arricchire i log di DHCP, DNS, NGFW, Radius, Switch, VPN, Wifi, Load Balancer...

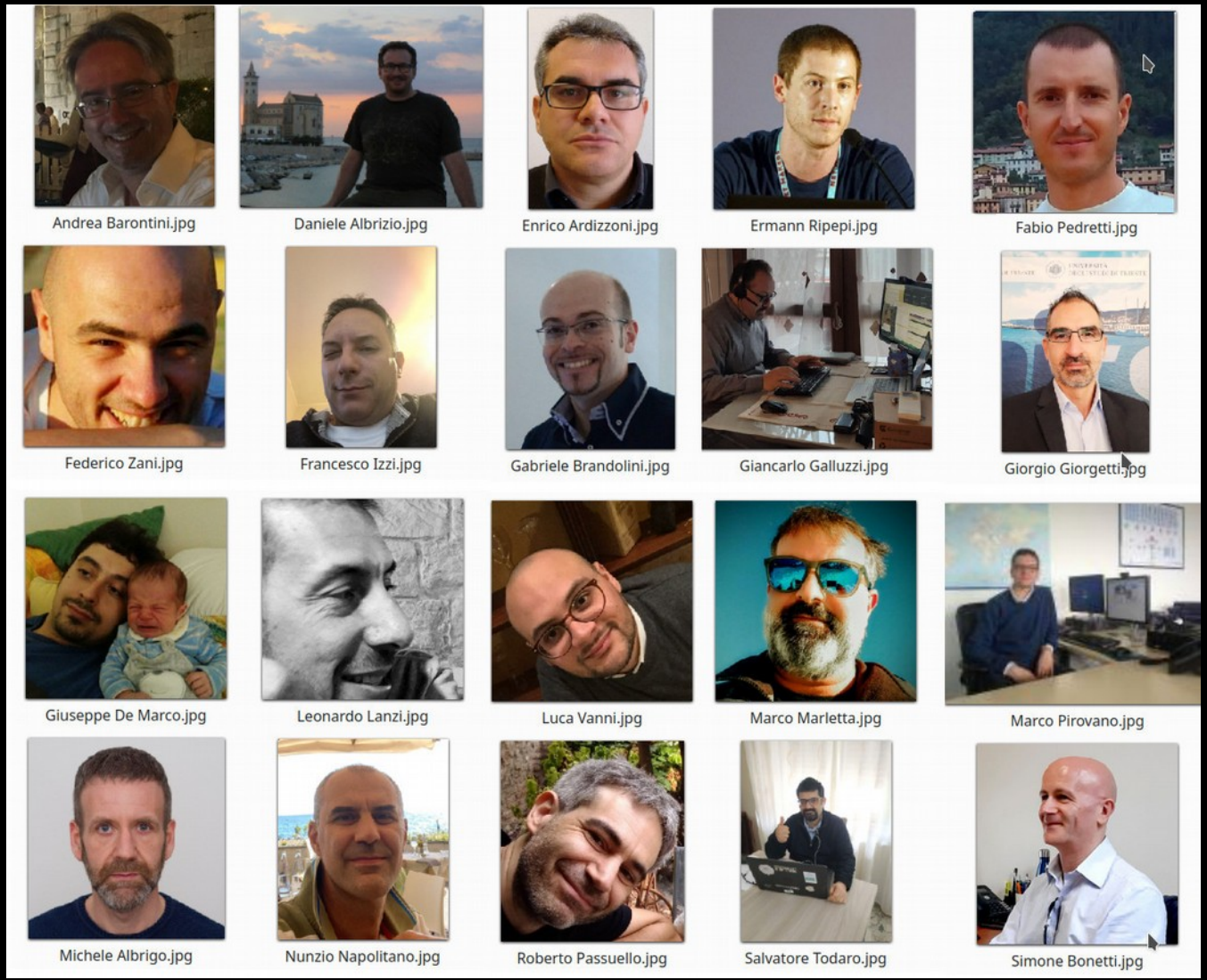
...ovviamente è tutto in officina, a disposizione di tutti!

conclusioni

- Più che “concludere” qualcosa, questa presentazione vuole essere un pit-stop, dal quale ripartire (più e meglio di prima)
- E quindi apriamo le porte del Bar è… invitiamo tutti (…*gli “operativi” amici del GPC*) a fare un salto:

N.B.: la porta resterà aperta tutt’oggi. Se entrate, cortesemente, presentatevi (nome, cognome, Ente di afferenza). Se la trovate chiusa, bussatemi: @Damiano_Verzulli (Telegram ; la mia porta è SEMPRE aperta!).

Quei brutti e cattivi banconisti...



Grazie!