wooclap.com
codice WSGARR25

WORKSHOP GARR 2025

NET MAKERS

Collaborazione fra università per il rilevamento di incidenti di sicurezza in contesti federati

Enrico Venuto
Politecnico di Torino

Damiano Verzulli
Università G. D'Annunzio di Chieti/Pescara

Antefatto

Politecnico di Torino

Il Politecnico di Torino ha di recente portato tutti i sistemi di autenticazione, ai servizi, anche cloud, ivi inclusi quelli di MS365 (Teams, SharePoint, Onedrive, Outlook365,..) su un IdP on-prem.

L'IdP diventa il punto unico di accesso a tutti i servizi dell'ateneo.

Si sono perse alcuni degli strumenti di security offerti da Microsoft relativamente alla sicurezza degli account e dei login.

Necessità di uno strumento per l'identity management e rilevazione incidenti per tutti i servizi dell'ateneo (e non solo quelli MS365).

Situazione di partenza

- Tutti i log dell'ateneo convergono su un remote syslog server
  - centralizzato
  - on-prem
  - gestito in segregation of duties

- il syslog alimenta un SIEM proprietario

- per mesi si è operato con strumenti «arcaici» di ricerca ed investigazione (script awk, bash, python, …)

Opportunità

L'*Università G. D'Annunzio di Chieti/Pescara* ha organizzato in giugno un tavolo tecnico per la condivisione di esperienze e scelte tecnologiche fatte da diverse università riguardo strumenti di virtualizzazione, infrastrutture di rete locale, ivi inclusi i temi dell'automazione.

Nei momenti di confronto/networking emerge un'esperienza di trattamento massivo di log effettuato in

- maniera moderna
- automatizzata
- facilmente replicabile
- basso impatto computazionale

Obiettivo

- Focus sul problema delle auth
- Visibilità di quanto accade
- **Evidenziare** possibili **anomalie** nei processi di autenticazione federata multifactor, single sign-on shibboleth di tutti i servizi di ateneo
- Produzione di dati di qualità per *«nutrire»* un nuovo SIEM/SOAR specializzato sull'Identity Management

Questione LOG: i log servono ad alimentare i sistemi SIEM/SOAR che altrimenti non potrebbero funzionare e soprattutto non sarebbero in grado di effettuare la detection di anomalie.

Obiettivo NIS

PR.PS-4: *I registri di log sono generati e resi disponibili per il monitoraggio continuo.*

- PR.PS-4.1: *Tutti gli accessi eseguiti da remoto e quelli effettuati con privilegi amministrativi sono registrati.*
- PR.PS-4.2: *Per almeno i sistemi informativi e di rete rilevanti, sono conservati in modo sicuro, e possibilmente centralizzato, almeno i log necessari ai fini del monitoraggio degli eventi di sicurezza, ivi compresi quelli relativi agli accessi di cui al punto PR.PS-4.1.*
- PR.PS-4.3: *In accordo agli esiti della valutazione del rischio, sono definite e documentate tempistiche di conservazione dei log di cui la punto PR.PS-4.2.*

DE.CM-1: *Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.*

- DE.CM-1.1: *Per almeno i sistemi informativi e di rete rilevanti, sono presenti, aggiornati, mantenuti e configurati in modo adeguato strumenti tecnici per rilevare tempestivamente gli incidenti significativi.*

Collaborazione

Vista l'esperienza di UdA nello sviluppo e sull'automazione di servizi e gestione code comunicata durante il tavolo tecnico, inizia una fattiva collaborazione.

La condivisione di visione (=> FLOSS + conoscenza libera) e la fiducia reciproca delle figure di riferimento ha innescato la dinamica di *collaborazione reale* del tutto *informale* e *sperimentale*, ma *concreta*.

Fattore abilitante: stack 100% "open-source" delle tecnologie utilizzate (e comunque liberamente disponibile a terzi).

Attività

Setup di ambiente collaborativo basato su Mattermost (Free Edition) e su GitLab on-prem (Community Edition).

Setup del sistema di log ingestion con sistema multi-coda modulare a microservizi.

Automazione della creazione dei microservizi (CI) e del relativo deploy con ansible (CD)

- Sistema completamente automatizzato che utilizza risorse minime
- Bonus: arricchimento via REST-API esterne per geo-referenziazione, risk-scoring e ricongiunzione identità

Attività

Setup dell'infrastruttura di ingestion dei log dell'IdP provenienti dal syslog (VM Ubuntu):

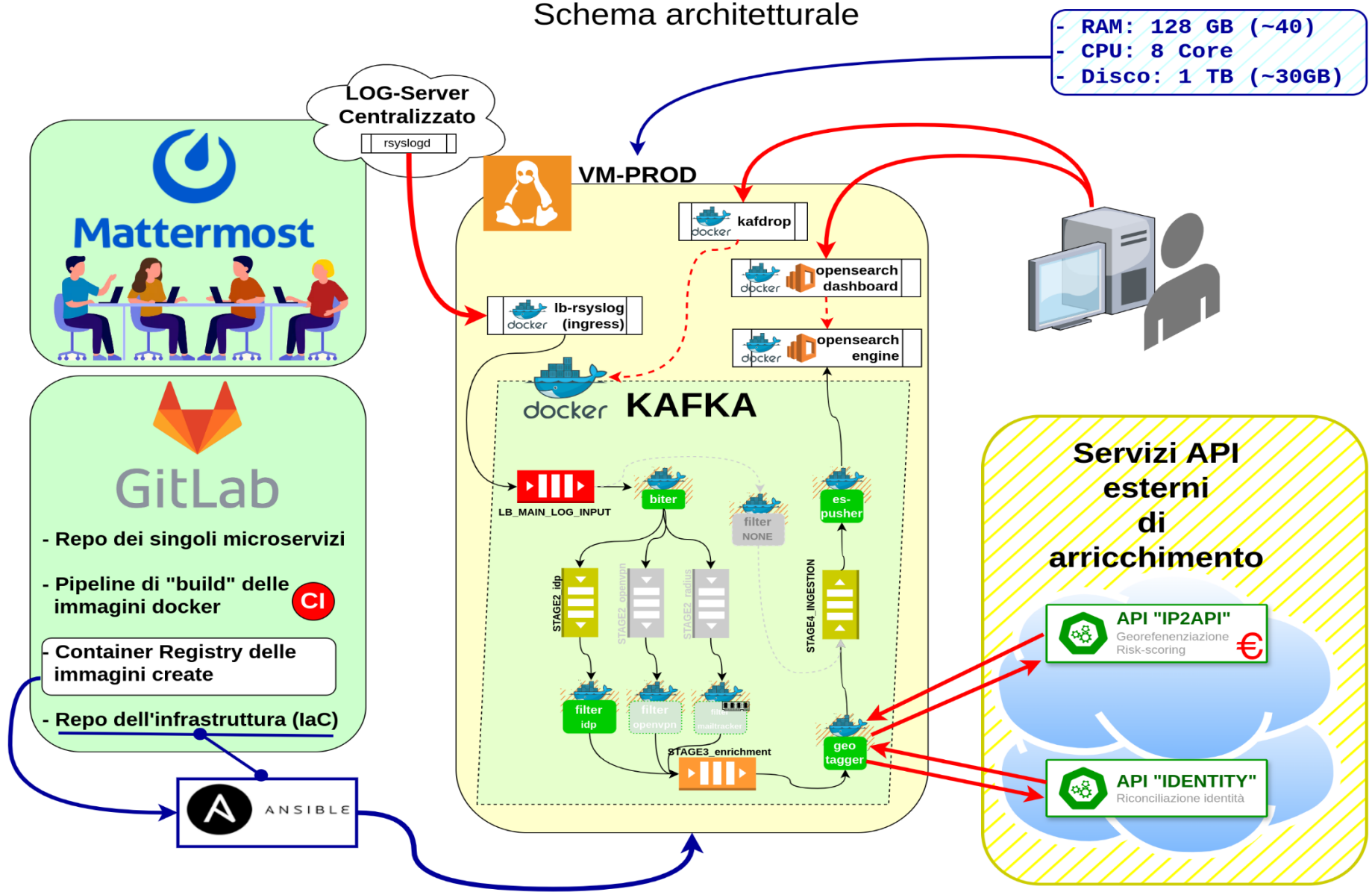
- filtrare gli eventi
- arricchire i log con altri dati
- inserire dati in OpenSearch
- realizzare cruscotti per la visualizzazione dati.

Attività in Roadmap

- Ingestion di altre fonti dati quali WiFi, Radius, acquisizione di log MS365, AD, …
- Adozione di un sistema di SIEM/SOAR integrato con l'OpenSearch esistente
- In valutazione sperimentazione di strumenti di IA per interrogazione e Anomaly Detection

LOG Biter @ PoliTO

Schema architetturale



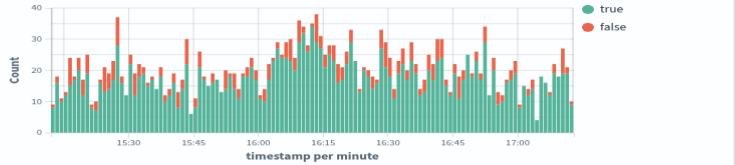
[AUTH-*] [numeri] auth TOT

2,471

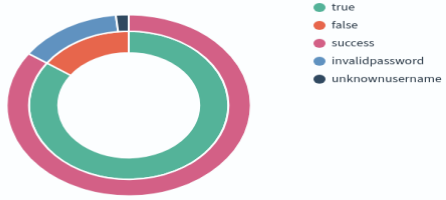
[AUTH-*] [numeri] auth_success / auth_fail

2,092	379
true - Count	false - Count

[AUTH-*] [Istogramma] auth success/fail > Time

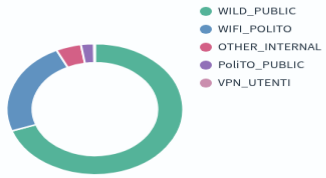


[AUTH-*] [Torta] auth_success >> auth_result

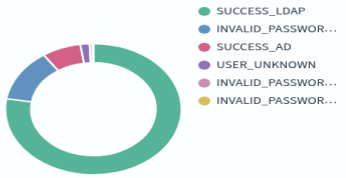


[AUTH-*] [Torta] auth_success >> sp

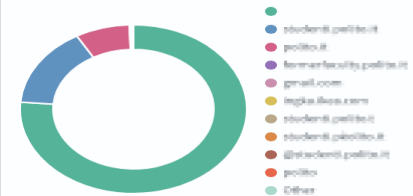
[AUTH-*] [Torta] ip_class



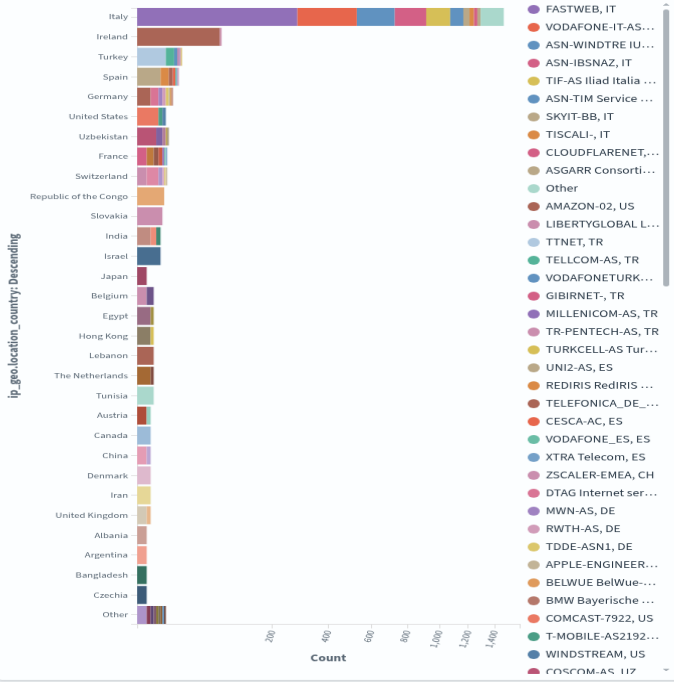
[AUTH-*] [Torta] Label



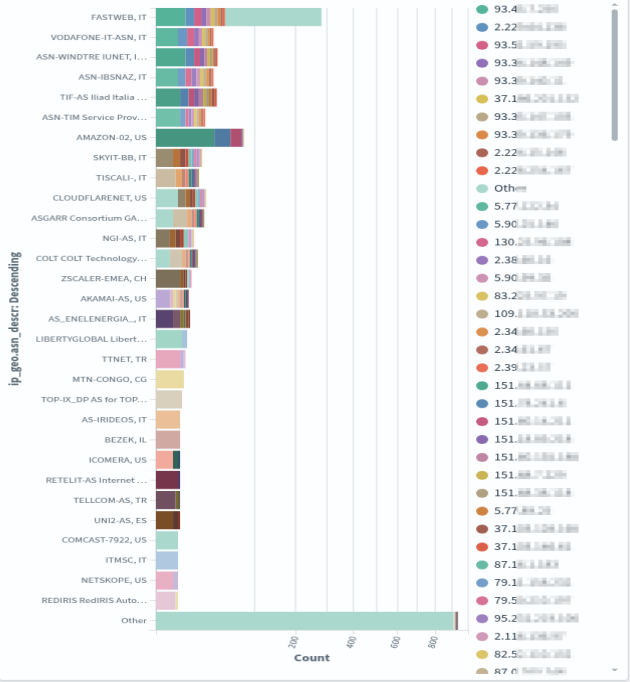
[AUTH-*] [Torta] realm



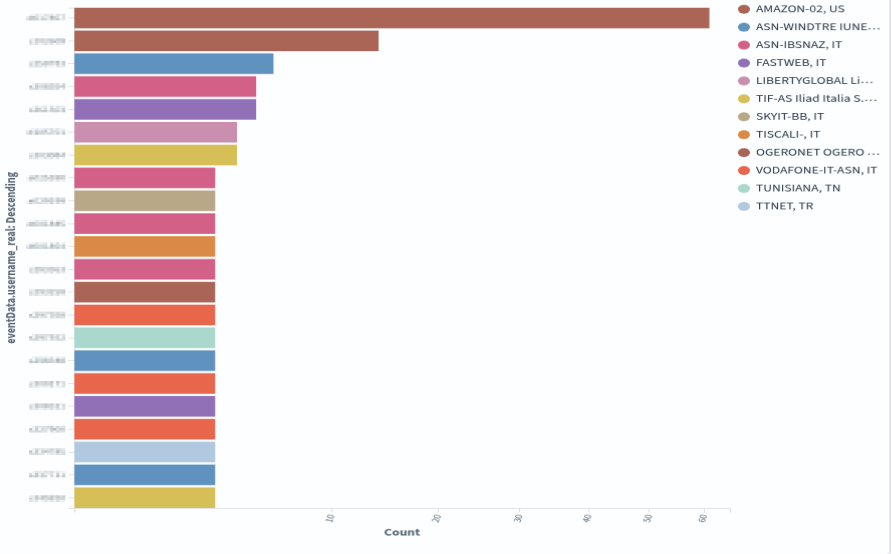
[AUTH-*][Istogramma] Country >> ASN



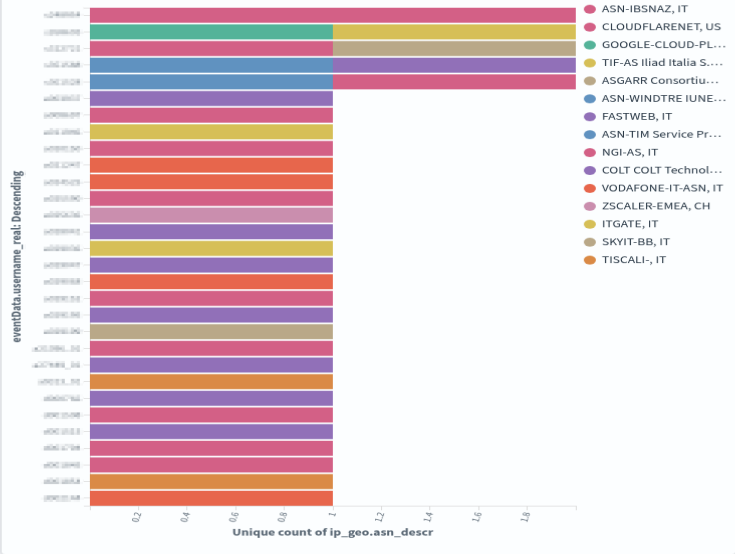
[AUTH-*][Istogramma] ASN >> IP



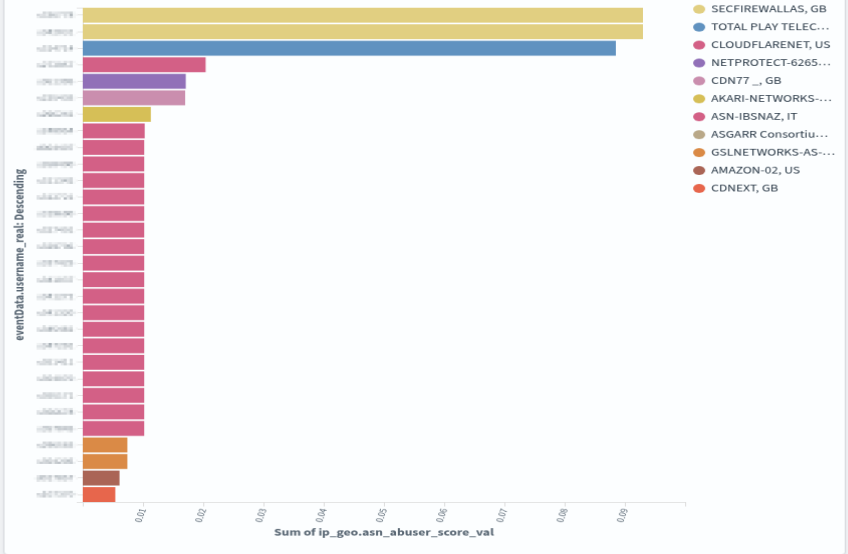
[AUTH-*][Istogramma] Utente >> num_login(asn)



[AUTH-*][Istogramma] Utente >>count(distinct(asn))



[AUTH-*][Istogramma] Utente >>sum(asn_score)



[AUTH*] [numeri] auth TOT

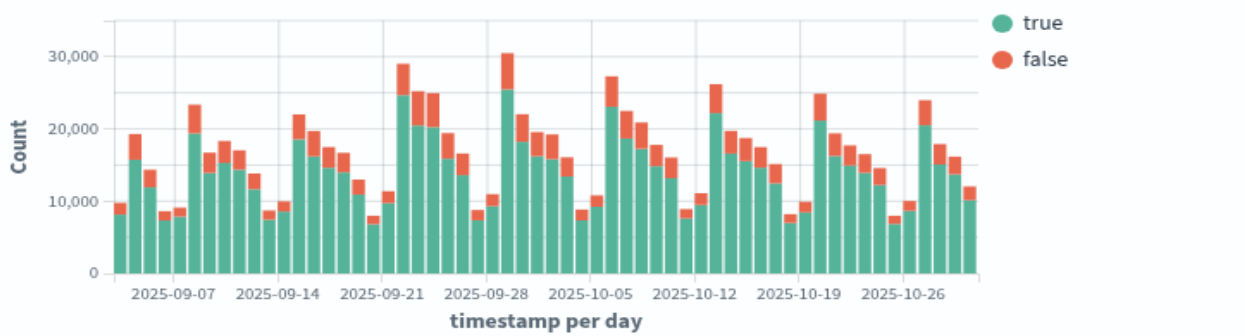
960,548

[AUTH-*] [numeri] auth_success / auth_fail

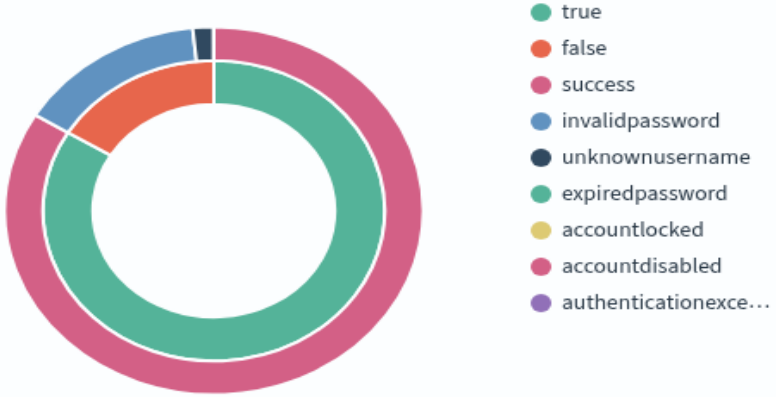
804,161 true - Count

156,387 false - Count

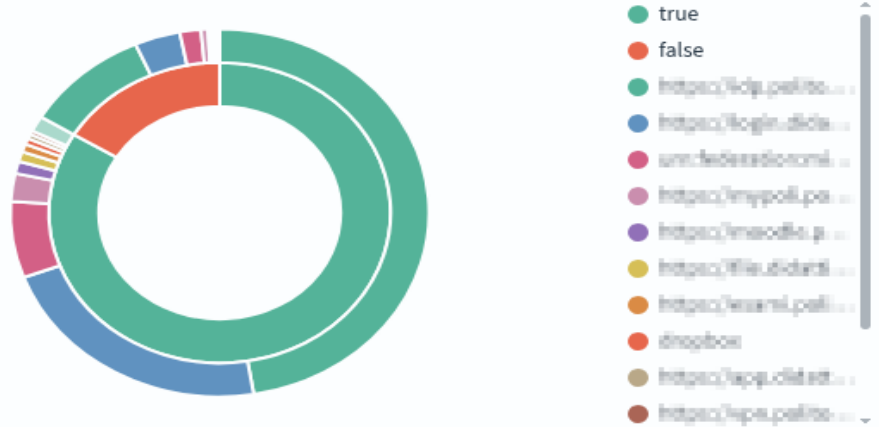
[AUTH-*] [Istogramma] auth success/fail > Time



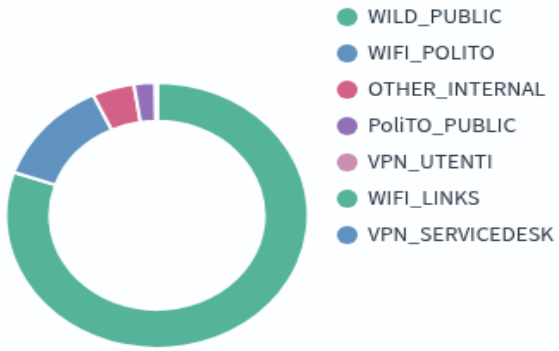
[AUTH-*] [Torta] auth_success >> auth_result



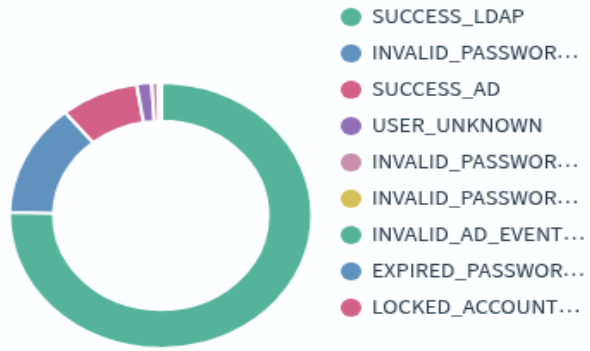
[AUTH-*] [Torta] auth_success >> sp



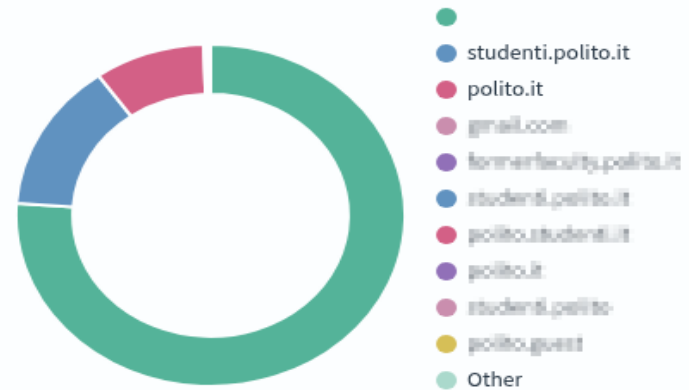
[AUTH-*] [Torta] ip_class



[AUTH-*] [Torta] Label

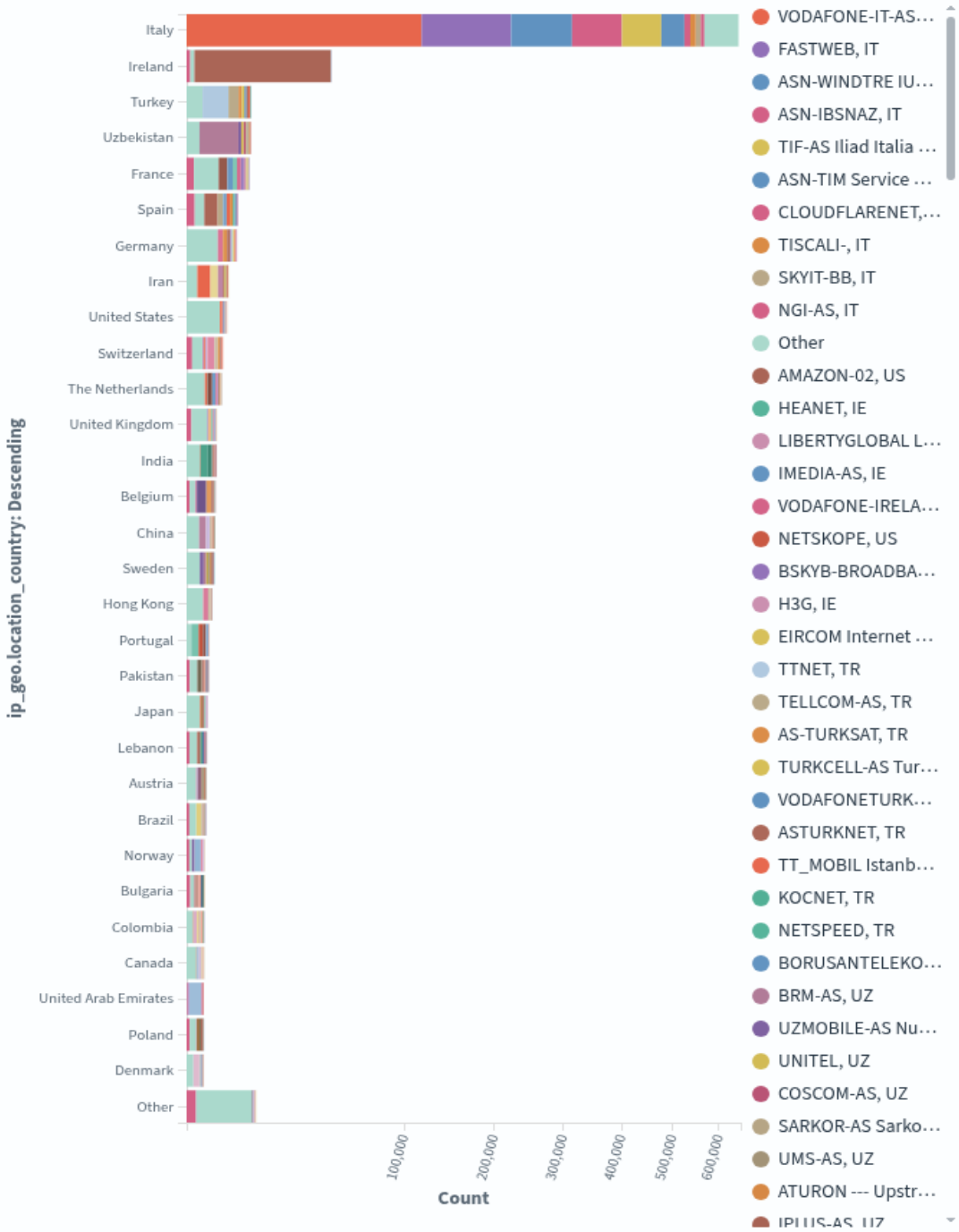


[AUTH-*] [Torta] realm

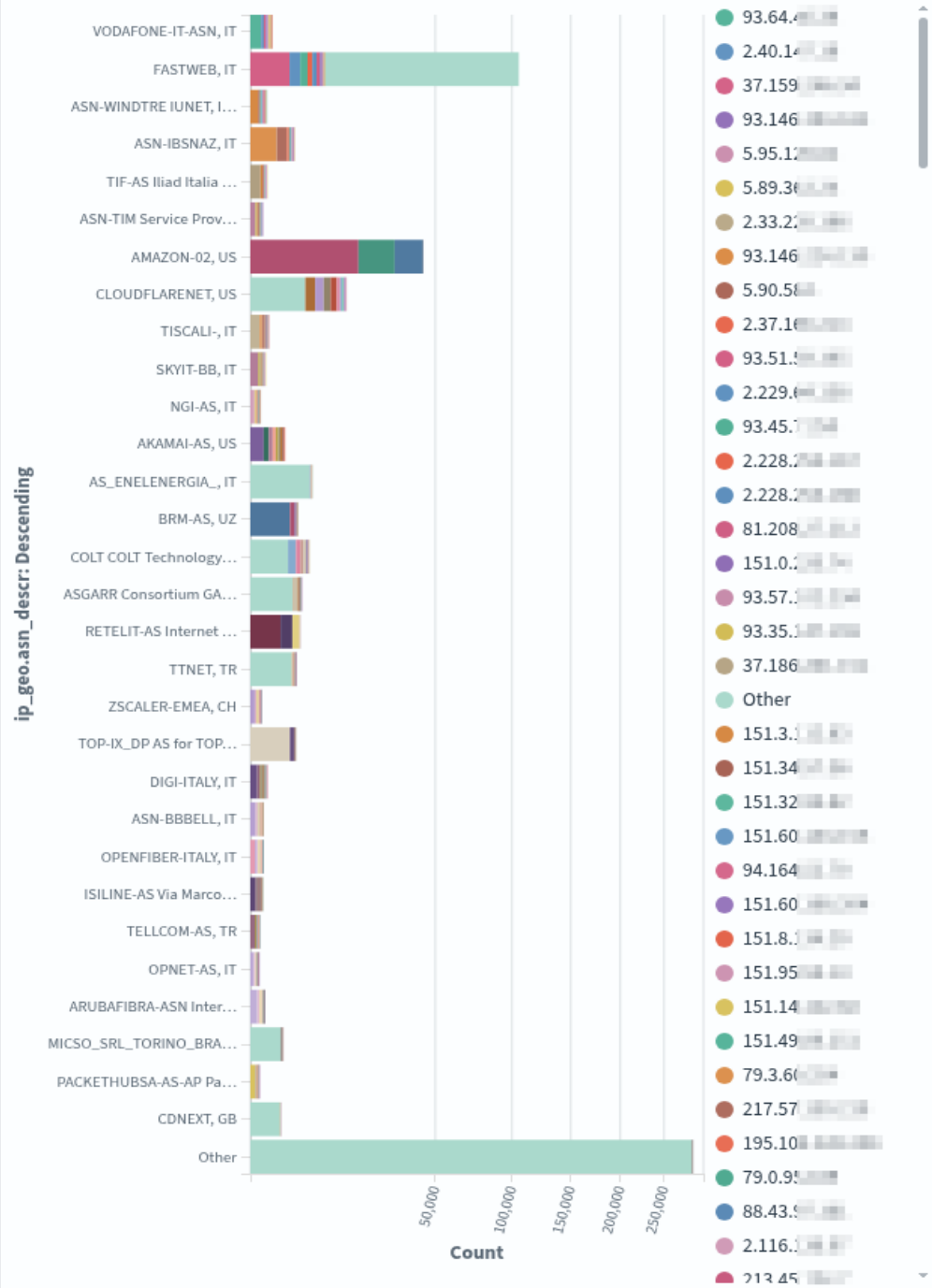


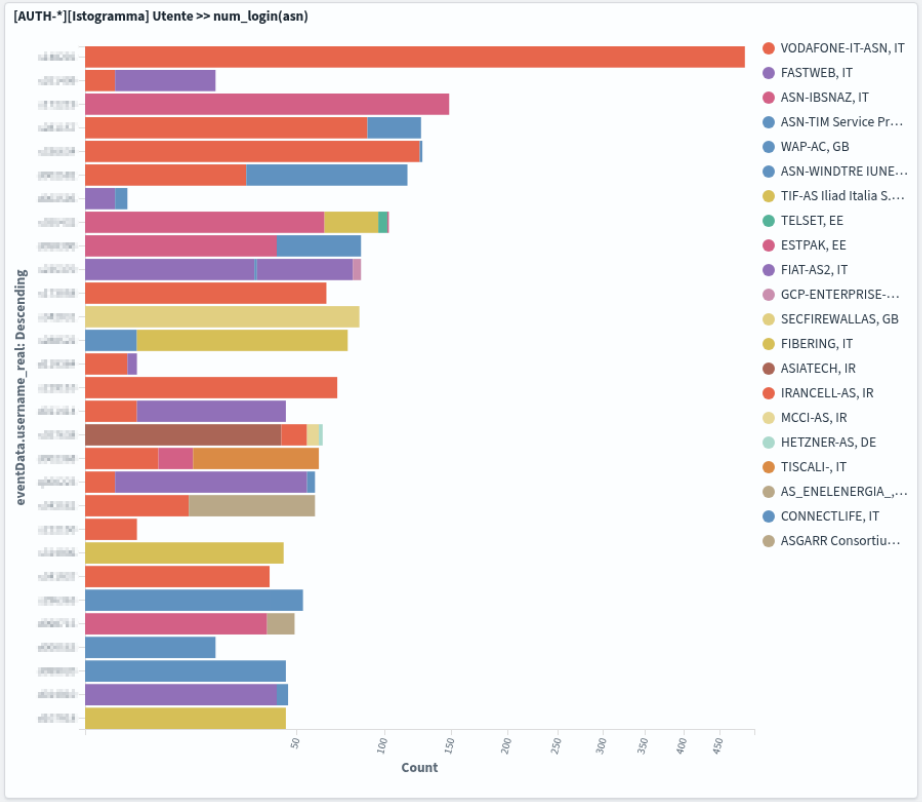
NET MAKERS

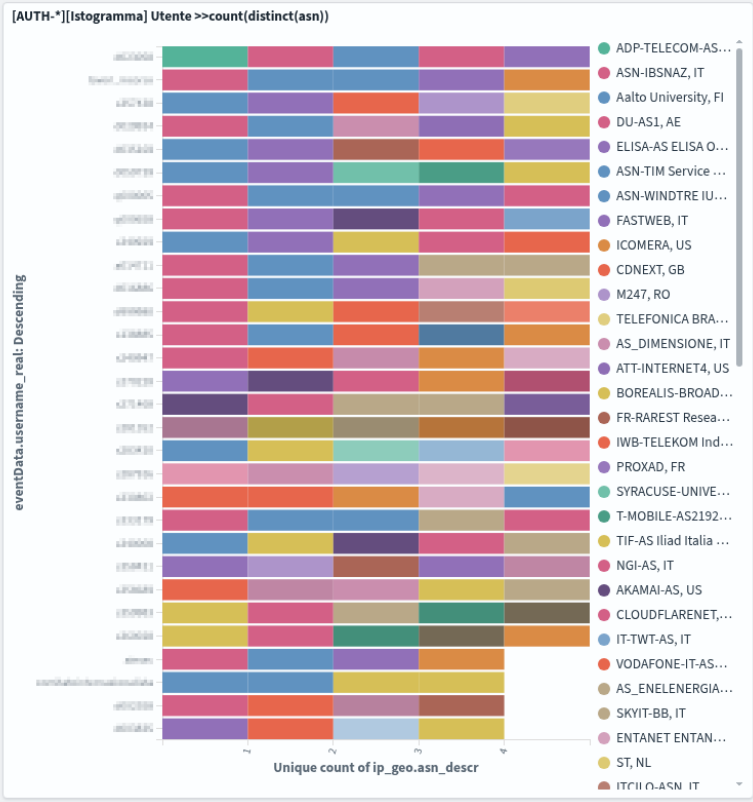
[AUTH-*][Istogramma] Country >> ASN

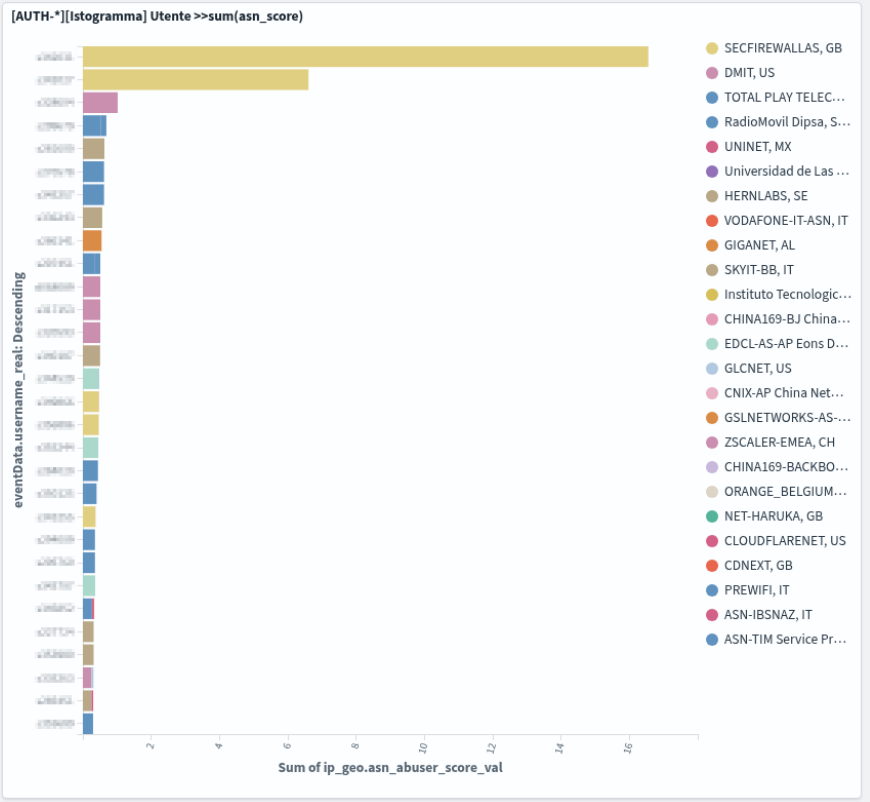


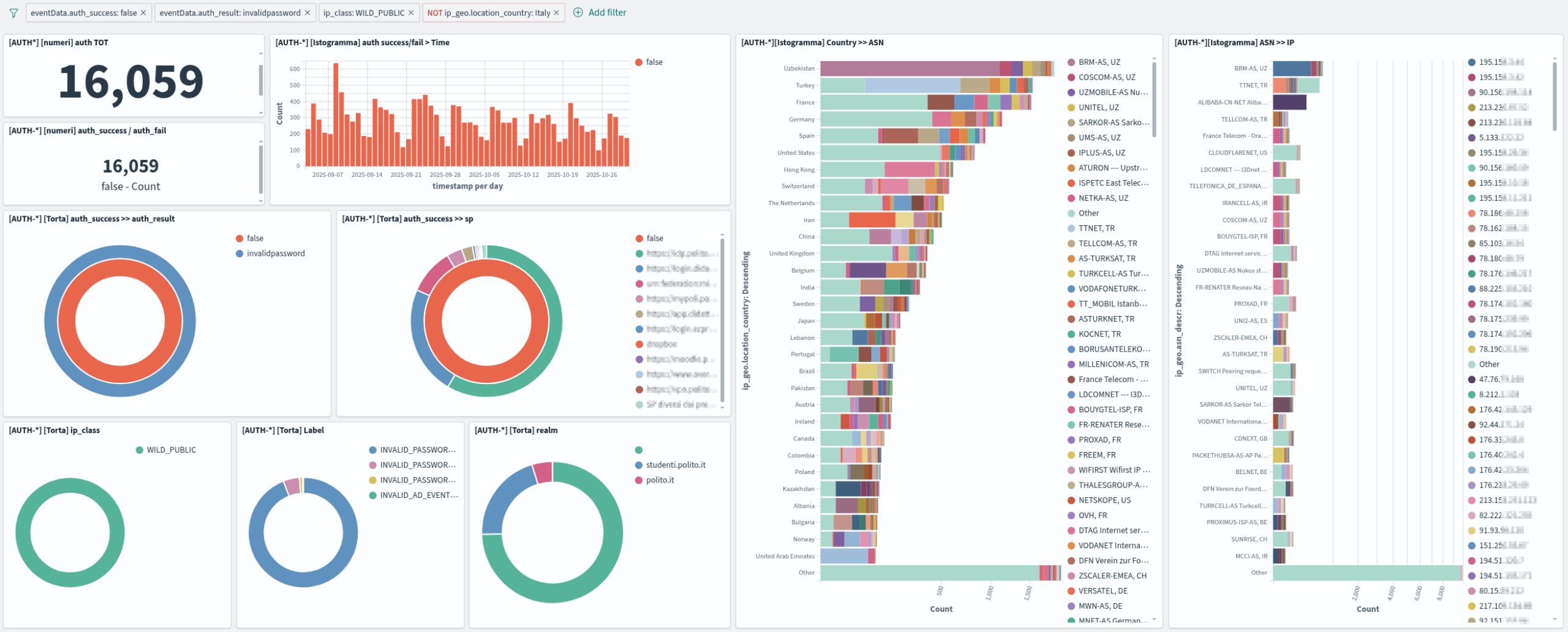
[AUTH-*][Istogramma] ASN >> IP



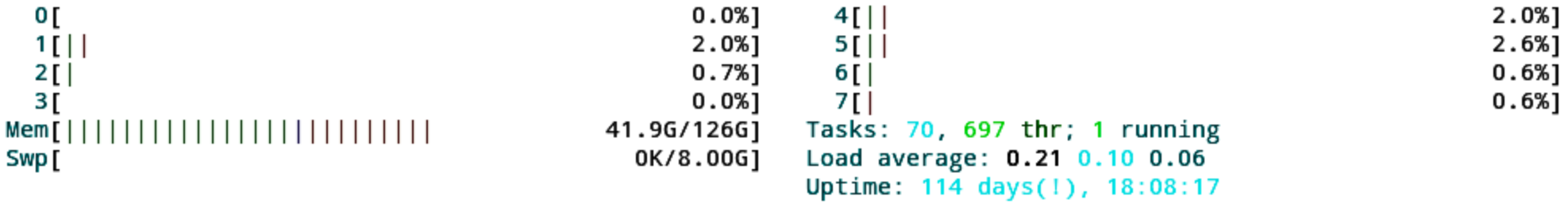

[AUTH-*][Istogramma] Utente >> num_login(asn)
eventData.username_real: Descending
Count
VODAFONE-IT-ASN, IT
FASTWEB, IT
ASN-IBSNAZ, IT
ASN-TIM Service Pr…
WAP-AC, GB
ASN-WINDTRE IUNE…
TIF-AS Iliad Italia S.…
TELSET, EE
ESTPAK, EE
FIAT-AS2, IT
GCP-ENTERPRISE-…
SECFIREWALLAS, GB
FIBERING, IT
ASIATECH, IR
IRANCELL-AS, IR
MCCI-AS, IR
HETZNER-AS, DE
TISCALI-, IT
AS_ENELENERGIA_,…
CONNECTLIFE, IT
ASGARR Consortiu…


[AUTH-*][Istogramma] Utente >>count(distinct(asn))
eventData.username_real: Descending
Unique count of ip_geo.asn_descr
ADP-TELECOM-AS…
ASN-IBSNAZ, IT
Aalto University, FI
DU-AS1, AE
ELISA-AS ELISA O…
ASN-TIM Service …
ASN-WINDTRE IU…
FASTWEB, IT
ICOMERA, US
CDNEXT, GB
M247, RO
TELEFONICA BRA…
AS_DIMENSIONE, IT
ATT-INTERNET4, US
BOREALIS-BROAD…
FR-RAREST Resea…
IWB-TELEKOM Ind…
PROXAD, FR
SYRACUSE-UNIVE…
T-MOBILE-AS2192…
TIF-AS Iliad Italia …
NGI-AS, IT
AKAMAI-AS, US
CLOUDFLARENET,…
IT-TWT-AS, IT
VODAFONE-IT-AS…
AS_ENELENERGIA…
SKYIT-BB, IT
ENTANET ENTAN…
ST, NL

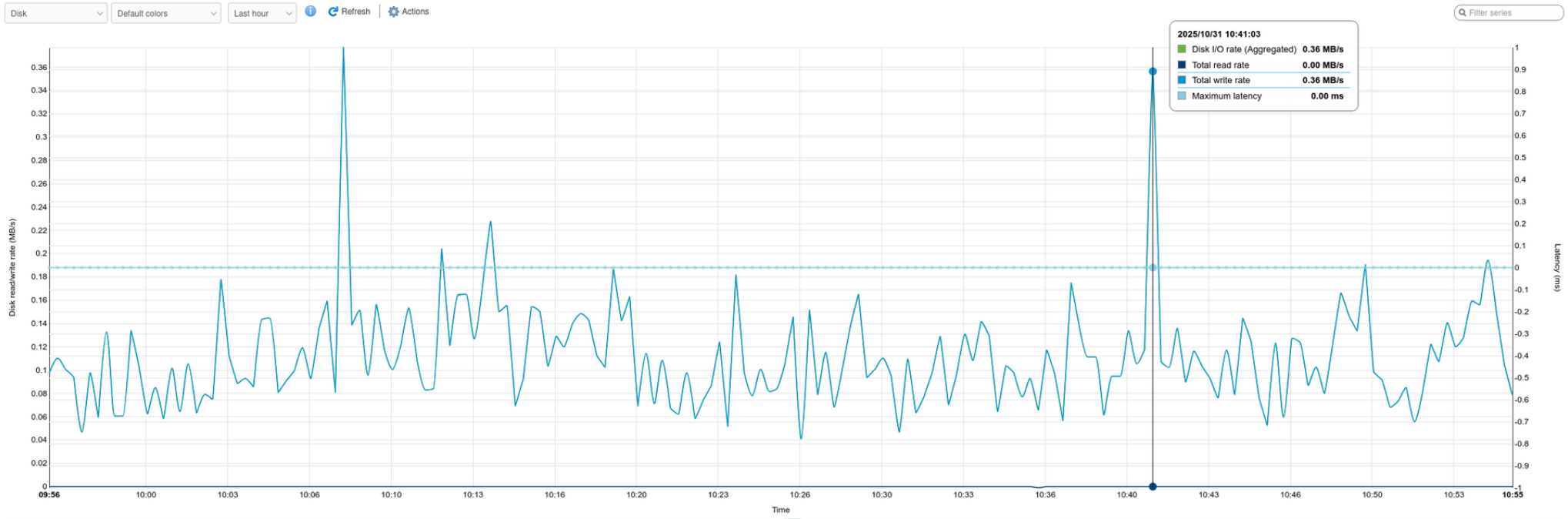

[AUTH-*][Istogramma] Utente >>sum(asn_score)
eventData.username_real: Descending
Sum of ip_geo.asn_abuser_score_val
SECFIREWALLAS, GB
DMIT, US
TOTAL PLAY TELEC…
RadioMovil Dipsa, S…
UNINET, MX
Universidad de Las …
HERNLABS, SE
VODAFONE-IT-ASN, IT
GIGANET, AL
SKYIT-BB, IT
Instituto Tecnologic…
CHINA169-BJ China…
EDCL-AS-AP Eons D…
GLCNET, US
CNIX-AP China Net…
GSLNETWORKS-AS-…
ZSCALER-EMEA, CH
CHINA169-BACKBO…
ORANGE_BELGIUM…
NET-HARUKA, GB
CLOUDFLARENET, US
CDNEXT, GB
PREWIFI, IT
ASN-IBSNAZ, IT
ASN-TIM Service Pr…


eventData.auth_success: false
eventData.auth_result: invalidpassword
ip_class: WILD_PUBLIC
NOT ip_geo.location_country: Italy
Add filter
[AUTH*] [numeri] auth TOT
16,059
[AUTH-*] [numeri] auth_success / auth_fail
16,059
false - Count
[AUTH-*] [Istogramma] auth success/fail > Time
false
Count
timestamp per day
[AUTH-*] [Torta] auth_success >> auth_result
false
invalidpassword
[AUTH-*] [Torta] auth_success >> sp
false
[AUTH-*] [Torta] ip_class
WILD_PUBLIC
[AUTH-*] [Torta] Label
INVALID_PASSWOR…
INVALID_PASSWOR…
INVALID_PASSWOR…
INVALID_AD_EVENT…
[AUTH-*] [Torta] realm
studenti.polito.it
polito.it
[AUTH-*][Istogramma] Country >> ASN
ip_geo.location_country: Descending
Count
BRM-AS, UZ
COSCOM-AS, UZ
UZMOBILE-AS Nu…
UNITEL, UZ
SARKOR-AS Sarko…
UMS-AS, UZ
IPLUS-AS, UZ
ATURON --- Upstr…
ISPETC East Telec…
NETKA-AS, UZ
Other
TTNET, TR
TELLCOM-AS, TR
AS-TURKSAT, TR
TURKCELL-AS Tur…
VODAFONETURK…
TT_MOBIL Istanb…
ASTURKNET, TR
KOCNET, TR
BORUSANTELEKO…
MILLENICOM-AS, TR
France Telecom - …
LDCOMNET --- I3D…
BOUYGTEL-ISP, FR
FR-RENATER Rese…
PROXAD, FR
FREEM, FR
WIFIRST Wifirst IP …
THALESGROUP-A…
NETSKOPE, US
OVH, FR
DTAG Internet ser…
VODANET Interna…
DFN Verein zur Fo…
ZSCALER-EMEA, CH
VERSATEL, DE
MWN-AS, DE
[AUTH-*][Istogramma] ASN >> IP
ip_geo.asn_descr: Descending
Count
Other

Sostenibilità



CPU/Memoria



Name	Unit	Average	Maximum	Minimum	Latest
Disk I/O rate (Aggregated)	MB/s	0.11	0.38	0.04	0.08
Total read rate	MB/s	0	0	0	0
Total write rate	MB/s	0.11	0.38	0.04	0.08
Maximum latency	ms	0	0	0	0

Disk I/O

Conclusioni

- Perso: Potente sistema proprietario che opera sui suoi servizi, non eccessivamente custom-izzabile
  (vedi es. throttling nelle ricerche e nei tempi di ritenzione)
- Guadagnato: Punto unico di autenticazione MFA, federato, multi tecnologia (username/password, SPID, CIE, X509,…) con sistema open sostenibile, completamente adattabile e configurabile per specifiche esigenze

La costruzione di strumenti condivisi è essenziale, soprattutto se nasce dal riuso di soluzioni ed architetture open con deploy automatizzato e contribuisce alla creazione di importanti sinergie di nuove idee e strumenti potenti e di una «vision collettiva»

Questa presentazione è stata realizzata esclusivamente con l'utilizzo di intelligenze naturali

wooclap.com
codice WSGARR25

Grazie

Enrico Venuto
Politecnico di Torino

Damiano Verzulli
Università G. D'Annunzio di Chieti/Pescara

WORKSHOP GARR 2025
NET MAKERS