PROCEDamus

PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI

progetto di formazione-intervento per le università e gli enti di ricerca



Best-practice: raccolta, analisi e conservazione di eventi di autenticazione: i casi di UniTS e di UniCH

Dr. Damiano Verzulli
Responsabile Divisione 9 - Informatica
damiano.verzulli@unich.it

Napoli, **Università "Parthenope"**, 08/10/2026

Contesto di riferimento

- 16 dipartimenti NdV
- 74 Corsi di Studio di 1° e 2° livello NdV
- 444 tecnici/amministrativi PIAO
- 21 Collaboratori linguistici PIAO
- 931 docenti e ricercatori (2024) MUR
- 20460 studenti (aa 2024/2025) MUR

Fonti:
NdV: Relazione annuale 2025 – Nucleo di Valutazione
PIAO: PIAO 2026-2028 – https://unich.it/trasparenza.it/index.php?id_sezione=4
MUR: https://ustat.mur.gov.it/dati/didattica/italia/atenei-statali/chieti-e-pescara



DIVISIONE 9 - INFORMATICA

- Settore Applicativi Servizi Studenti
- Settore Gestione Web di Ateneo e Siti Federati
- Settore Help Desk Informatico di Ateneo
- Settore Reti, Sistemi e Posta Elettronica
- Settore Statistiche di Ateneo e Banche Dati - Applicativi Didattica, Ricerca e Terza Missione
- Settore Sviluppo e Manutenzione Applicativi
- Settore Teledidattica, E-Learning, Videoconferenze e Sistemi Cloud
- Settore Telefonia



La "Divisione Informatica" è qui dentro. Riorganizzata nel 2024 oggi è strutturata così ⇒

Cos’é un LOG...

- Negli ultimi anni (~20) il termine “LOG” è uscito dagli ambiti tecnici e si è diffuso in contesti diversi, soprattutto giuridici (Uffici Legali, Autorità) e amministrativo/manageriali (linee dirigenziali aziendali);
- Anche all’interno della comunità “tecnica”, l’utilizzo del termine si è diffuso enormemente.
- Tuttavia...

...in pochissimi, anche fra gli addetti ai lavori, “trattano” LOG o ne hanno mai visto qualcuno, realmente!



Ripartiamo dalle basi: ***cos’è REALMENTE un “LOG”?*** ⇒

Cos’é un LOG...

- Una riga di LOG non è niente altro che del semplice TESTO prodotto esplicitamente da un software in occasione di un qualche evento degno di nota.
  Ad esempio:

```
Sep 20 21:35:27 LEVEL=local6.info TAG=imapd: MESSAGE= LOGIN, user=damiano.verzulli, ip=[::ffff:83.225.55.235], port=[11978], protocol=IMAP
```

```
Sep 20 21:35:27
LEVEL=local6.info
TAG=imapd:
MESSAGE= LOGIN, user=damiano.verzulli, ip=[::ffff:83.225.55.235], port=[11978], protocol=IMAP
```

```
LOGIN
user=damiano.verzulli
ip=[::ffff:83.225.55.235]
Port=[11978]
protocol=IMAP
```

Damiano…
...alle 21:35 del 20/09…
...era connesso ad una rete VODAFONE…
...ed ha acceduto alla posta



Cos'é un LOG...

Che dicono in queste tre righe?

```
Sep 20 21:42:19 LEVEL=mail.info TAG=postfix/qmgr[70743]: MESSAGE= 998881DF8FE: from=<damiano.verzulli@unich.it>, size=15774, nrcpt=2 (queue active)

Sep 20 21:42:19 LEVEL=mail.info TAG=postfix/relay/smtp[3780328]: MESSAGE= 998881DF8FE: to=<daniele.romito@unich.it>, relay=10.0.49.213[10.0.49.213]:25, delay=0.62, delays=0.58/0/0/0.04, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 24FC01DFA1F)

Sep 20 21:42:19 LEVEL=mail.info TAG=postfix/relay/smtp[3780328]: MESSAGE= 998881DF8FE: to=<luigi.fagnano@unich.it>, relay=10.0.49.213[10.0.49.213]:25, delay=0.62, delays=0.58/0/0/0.04, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 24FC01DFA1F)
```



- Che è stata inviata una mail:
  da damiano.verzulli@unich.it
  a daniele.romito@unich.it e luigi.fagnano@unich.it;
- Che è successo alle 21:42:19 del 20/09
- Che la mail "pesava" 15774 byte;
- Che la mail è stata recapitata (*status=sent*) (~);
- Che ulteriori dettagli si possono recuperare mediante due ID (998881DF8FE e 24FC01DFA1F)

Cos’é un LOG...

```
Sep 16 13:18:21 LEVEL=daemon.notice TAG=radiusd[1290555]: MESSAGE= (6097084)   Login OK: [098915@unich.it] (from client ap_chieti port 0
cli 9C-DD-CC-AA-BB-CA via TLS tunnel)
```



- Che il 16/09, alle 13:18:21…
- ...lo username “098915@unich.it” si è connesso ad “eduroam”...
- ...da un access-point del campus di Chieti (ap_chieti)…
- ...con un device con MAC-Address 9C-DD-CC-AA-BB-CA…
- ...e che l’autenticazione è andata a buon fine (Login OK ; password corretta)

Cos’é un LOG...

```
20-09-2026 13:30:14.926 [API-STATS-GW] info: [telemetry/frontend] GET /get-cruscotto-iscritti-by-anno-accademico/2026 uid=098915 status=304 start=2026-09-20T13:30:14.333Z end=2026-09-20T13:30:14.926Z duration=593ms

20-09-2026 13:30:29.306 [API-STATS-GW] info: [telemetry/backend] GET https://api-xxx.internal.unich.it//get_cruscotto_iscritti_by_anno_accademico?anno=2025 status=200 start=2026-09-20T13:30:22.891Z end=2026-09-20T13:30:29.306Z duration=6415ms
```

- Che il 20/09/2026, alle 13:30:14.926…
- ...c’e’ stato un accesso web dell’utente 098915 a /get-cruscotto-iscritti-by-anno-accademico/2026
- ...che il server (frontend) ha evaso il tutto in 0.593 s

- Che il 20/09/2026, alle 13:30:20.306…
- ...un server (backend) ha recuperato /get_cruscotto_iscritti_by_anno_accademico?anno=2025 con successo (status=200)
- ...che il tutto è durato 6415ms



LOG: perché viene generato?

- Non esiste una definizione rigorosa di "**evento DEGNO DI NOTA**". Sono gli sviluppatori (delle applicazioni) a decidere quali sono gli eventi… degni di nota (...per le proprie applicazioni);
- In generale, possono essere classificati in macro-categorie:
  - Utilizzo di un determinato servizio da parte di un utente o di un sistema terzo ⇒ **LOG "di ACCESSO"**;
  - Azione svolta da una componente software, oppure da un dispositivo hardware ⇒ **LOG "di ATTIVITÀ"**;
  - Segnalazione di un errore o di una condizione anomala ⇒ **LOG "di ERRORE"**;
  - Messaggio informativo ⇒ **LOG "INFORMATIVI"**;

Avevamo detto che...

"Una riga di LOG non è niente altro che del semplice TESTO prodotto esplicitamente da un software in occasione di un qualche evento ***DEGNO DI NOTA****."*

I messaggi di LOG vengono generati per consentire la ricostruzione delle attività svolte dal software

LOG: perché viene raccolto e conservato?



- Da sempre (...ben prima della comparsa delle tematiche legate a “privacy” e/o “sicurezza”) i LOG vengono raccolti per poter supportare gli helpdesk nelle attività di supporto all’utenza.
  - “*La rete non va: non riesco a collegarmi al wifi!*”
  - “*La posta non funziona! Mi hanno spedito un messaggio che non mi è arrivato!*”
  - “*Non posso lavorare (da remoto)! Il protocollo elettronico non funziona!*”
  - “*Il computer non funziona! Metto la password, ma non succede nulla!*”

Per consentire ad un helpdesk di aiutare l’utente a risolvere questi (...e altri) problemi, è fondamentale avere accesso ai LOG prodotti dai componenti software con cui l’utente ha a che fare.

Senza LOG siamo “ciechi” e dobbiamo affidarci alle “palle di cristallo”!

LOG: perché viene raccolto e conservato?

- Consentire *REALMENTE* ad un “helpdesk” di supportare realmente l’utente nella risoluzione del problema… presta il fianco a **diversi aspetti reciprocamente contrapposti:**

DATI PERSONALI
i LOG devono necessariamente riportare dati relativi all’utenza dei servizi (e quindi: dati personali)

(riga di) LOG “TUTTO O NIENTE”
le tecnologie di produzione e raccolta di LOG non prevedono sistemi “nativi” per limitare l’accesso ai dati personali inclusi nei log



LOG (server) “TUTTO O NIENTE”
Storicamente, gli “amministratori di sistema” (e solo loro) avevano accesso a (tutti) i LOG.
Gli staff di supporto, potevano rivolgersi a loro o, in alternativa, chiedere di essere elevati a amministratori

Gestione dei LOG: recap

Dunque… abbiamo detto che i LOG sono:

- essenziali per il supporto utenti;
- ...e quindi, spesso, inscindibili dall'identità dell'utente che li ha generati;
- essenziali per la manutenzione delle infrastrutture (hardware/software);
- Rigidi nella struttura

AUMENTO COMPLESSITÀ

L'aumento progressivo dell'attenzione nei confronti dei "dati personali" ha comportato un altrettanto progressivo aumento della complessità del "trattamento" di queste informazioni.

ELEMENTI SEMPRE PIÙ CRITICI

Principali elementi attenzionati dal GPDP (a tutela dei lavoratori):

- Postazione di lavoro (MAC; IP)
- Navigazione Internet
- Posta Elettronica

Numerosi provvedimenti

(...ma io sono particolarmente affezionato ad uno specifico: il 5408460 del 2016)

OT (ma non tanto): il Provvedimento 5408460 del 2016

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VEDI ANCHE: Newsletter del

[do

Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro - 13 luglio 2016

Registro
n. 303

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresid
Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il d.lg

VISTE le s
D'Annunzio"

VISTE le Li
marzo 2007

ESAMINAT

VISTE le oss

RELATORE

Garante vs. Università "d'Annunzio"

"dichiarazione di illecito trattamento" (ambito "MAC Address")

1. E' stata lamentata da parte del personale dell'Università degli studi "G. D'Annunzio" di Chieti e Pescara la violazione
materia di protezione dei dati personali con riguardo, tra l'altro, all'asserito controllo posto in essere dal datore di lavoro i
di sistemi di comunicazione elettronica e di videosorveglianza.

TRIBUNALE DI CHIETI
SENTENZA A VERBALE
EX ART. 281 SEXIES C.P.C.
In nome del Popolo Italiano

NN. R.G. 715/2022 – 2015/22

ANNULLA

il provvedimento del GARANTE PER LA PROTEZIONE DEI DATI PERSONALI – meglio indicato in motivazione – impugnato nel presente giudizio dalla UNIVERSITÀ DEGLI STUDI DI CHIETI

il GARANT in favore della ese che liquida o e della marca tre il 15% sui compensi, per rimborso forfettario delle spese di lite ed altri accessori di legge; per il giudizio di Cassazione, nella somma di €. 2935,00 per compensi, oltre il 15% sui compensi, per rimborso forfettario delle spese di lite ed altri accessori di legge.

Tribunale di Chieti

Sentenza 23/10/2023

PONE

le spese della CTU espletata nel giudizio di merito a carico definitivo del GARANTE PER LA PROTEZIONE DEI DATI PERSONALI.

Alla Cancelleria per quanto di sua competenza.

Gestione dei LOG: recap

Rispetto a:

- […] inscindibili dall'identità dell'utente che li ha generati;
- essenziali per la manutenzione delle infrastrutture (hardware/software);

COMPLESSITÀ in ulteriore aumento

Il recente innalzamento del livello di attenzione in ambito "cyber" (fra le altre, NIS2), ha comportato un ulteriore aumento della complessità del "trattamento" di queste informazioni, anche rispetto ai tempi di reazione (ordine delle "ore")

Principali ELEMENTI "CYBER"

Principali elementi attenzionati dalla norma:

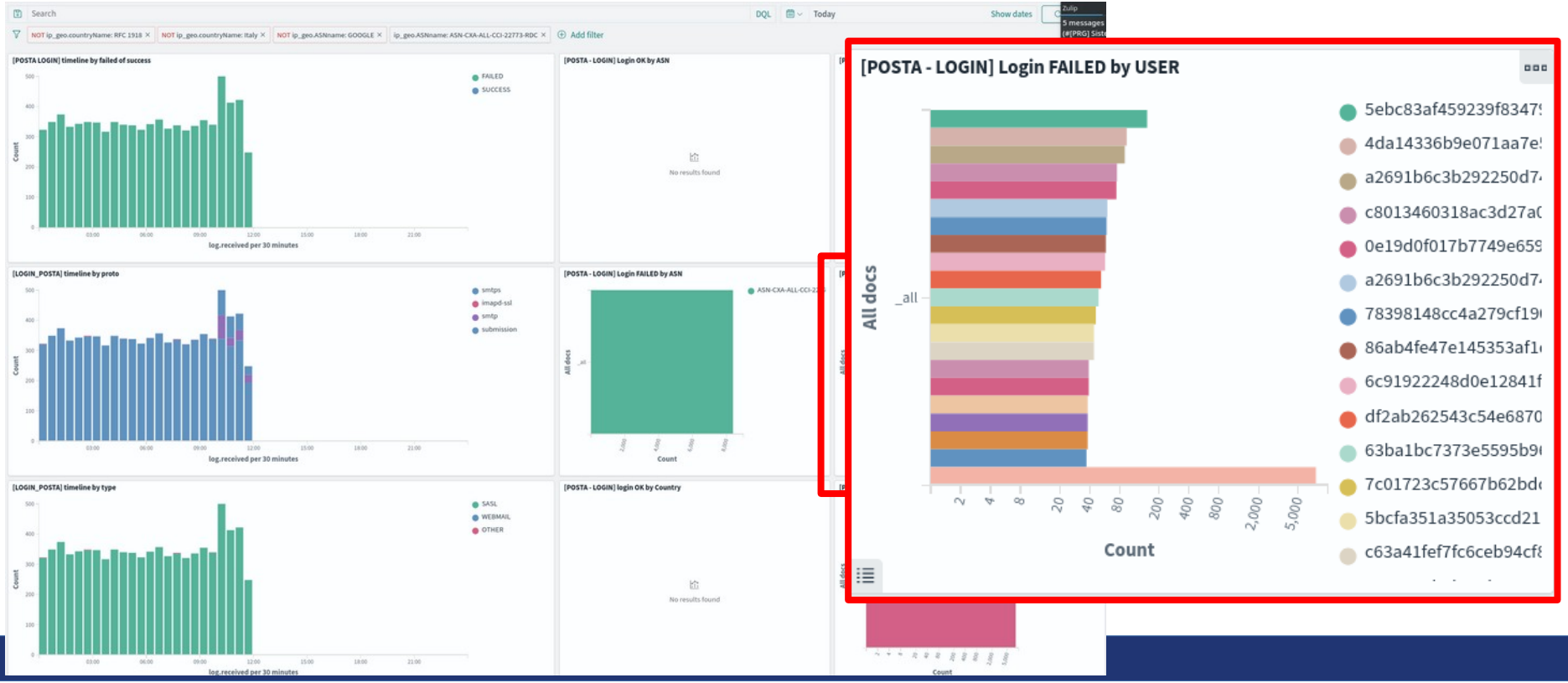
- Utilizzo fraudolento delle infrastrutture HW/SW
- Accessi non autorizzati (a HW, SW… e informazioni)
- regolamentazione/organizzazione

I LOG nel day-by-day: esempi concreti

Un paio di scenari reali… resi visibili soltanto grazie alla **raccolta** ed alla **analisi** dei LOG...

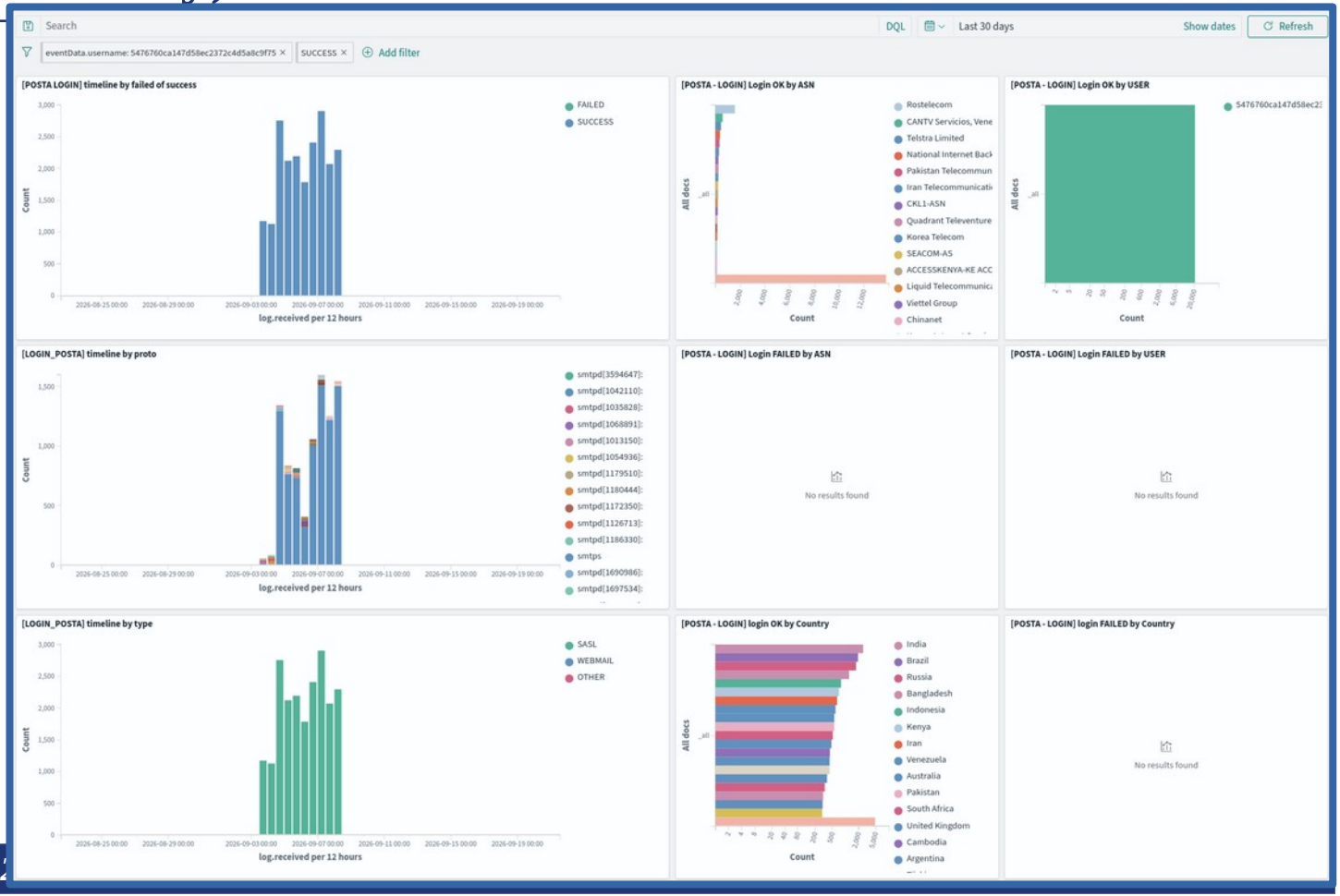
LOG (& security)

~8000 accessi FALLITI, da un singolo provider USA, per una pluralità di utenti, a partire da mezzanotte… (ed è ~mezzogiorno)



LOG (& security)

Un singolo utente, che nell'arco di qualche giorno (su un mese) invia ~20.000 mail… da una pluralità di paesi (extra-ue)...



I LOG a supporto dell'HelpDesk @UniCH

A partire da 01/2024, in Università "d'Annunzio" è stata avviata una significativa riorganizzazione del processo di **RACCOLTA**, **ARCHIVIAZIONE** e **CONSULTAZIONE** dei LOG.

L'obiettivo era di renderli disponibili al personale dell'HelpDesk in modo "compliant" alla normativa vigente:

- sia in termini di "minimizzazione" del trattamento (privacy by-design);
- sia in termini di "sicurezza" (profilazione e accounting degli accessi).

L'attività ha portato allo sviluppo di un "Pannello di Controllo" (in costante evoluzione) a disposizione del personale dell'HelpDesk

Log (& HelpDesk) - admin/L1

L’operatore riceve una chiamata da **Damiano Verzulli** per un problema di posta.

Dal “pannello” recupera le informazioni sull’account **damiano.verzulli**

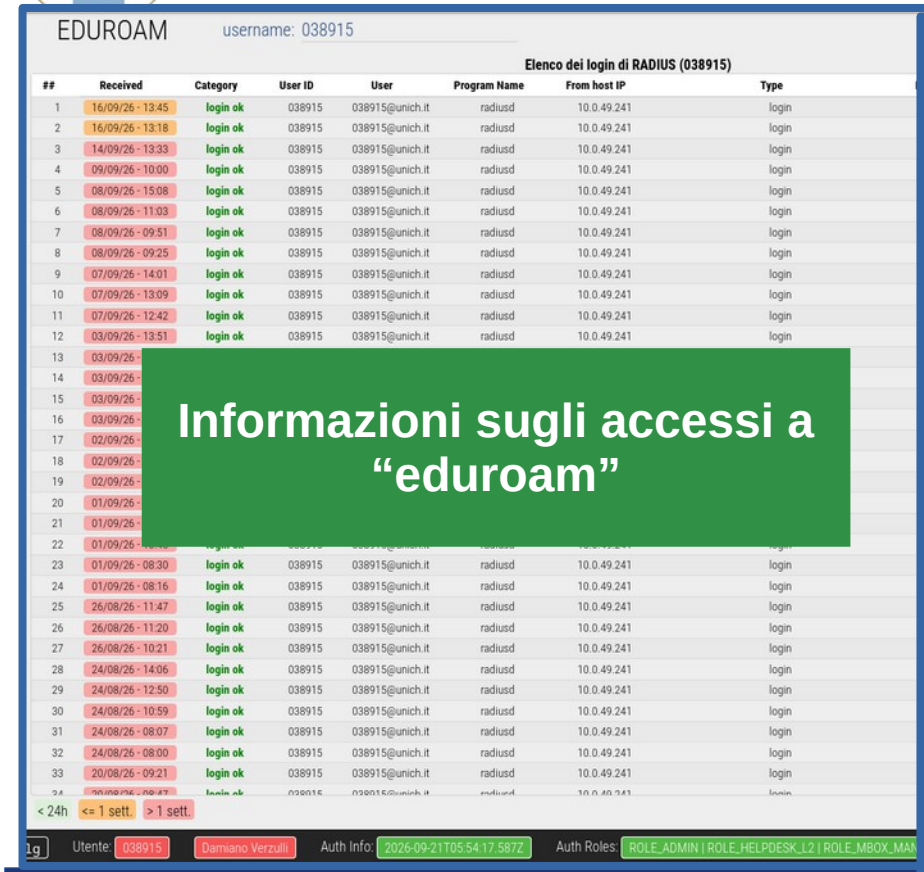


Log (& HelpDesk) - admin/L2

Il “Capo Settore” – *eventualmente ingaggiato per “escalation” del problema* -- ha accesso ai dati personali ed ha possibilità di intervento sul sistema



Log (& HelpDesk) – eduroam/VPN (connettività)





Conclusioni… e proposta

Abbiamo constatato che la raccolta dei LOG:

- è elemento **imprescindibile** per garantire l'operatività delle infrastrutture e dei servizi;
- è elemento **determinante** per garantire SLA adeguati in termini di "supporto utenti";
- è **prerequisito** per l'organizzazione di qualsiasi attività cyber-related

COMPLESSITÀ e CRITICITÀ

Un Ateneo medio/piccolo non può materialmente affrontare il tema autonomamente, a causa di un mix di fattori quali organico, complessità tecnica, tassi di evoluzione tecnologica/normativa, impatto sul resto dell'organizzazione



Perché non sviluppare delle "Linee Guida" condivise, non solo a livello tecnico, ma anche a livello "organizzativo", da rendere disponibile a chi lo desidera? …e magari condividendo anche know-how e applicativi?

Ringraziamenti

È tutto!

Grazie per l’attenzione!

Domande?

Dr. Damiano Verzulli
Responsabile Divisione 9 - Informatica
damiano.verzulli@unich.it