PROCEDamus

PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI

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



Sh@rePro e Sh@Tech: Best-practice su raccolta, analisi e conservazione eventi di autenticazione

Daniele Albrizio Università degli Studi di Trieste

Damiano Verzulli Università degli Studi "G. d'Annunzio" Chieti – Pescara

Napoli, 8 ottobre 2026

UNIVERSITÀ DEGLI STUDI DI TRIESTE

Sh@rePro e Sh@Tech: Best-practice su raccolta, analisi e conservazione eventi di autenticazione

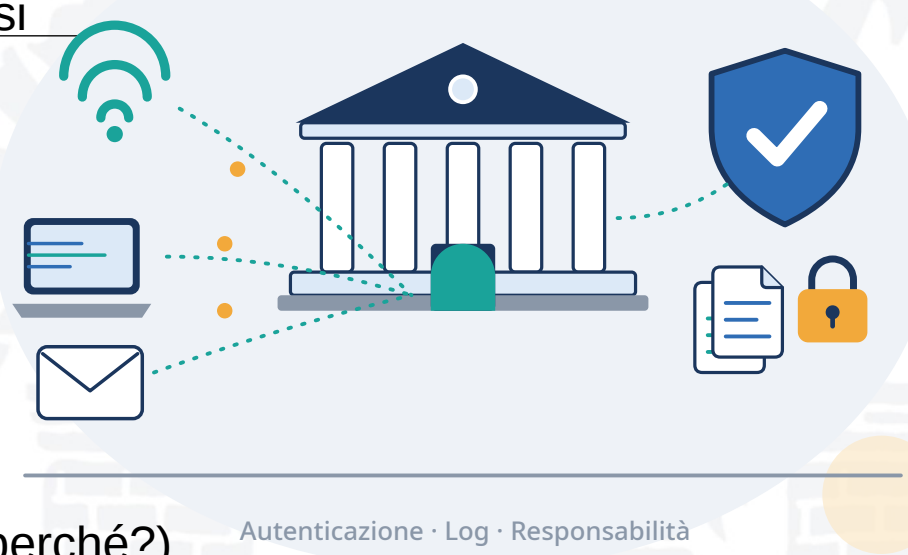
Introduzione allo scenario

8 ottobre 2026

Napoli

Daniele Albrizio

Ufficio Reti e telefonia



- Di che dati parliamo? Che dati ci servono?
- Autenticazione
  - Autenticazione:
    - Chi è? (E chi ha cambiato queste informazioni e quando/perché?)
  - Autorizzazione:
    - Chi può fare cosa? (Chi ha cambiato queste condizioni e quando/perché?)
  - Accounting:
    - Chi e quando ha fatto cosa?
- (NIST, NIS2, misure minime AgID)

Log ↔ Registro

- Non ha senso autenticare senza tenere un registro degli accessi e, in taluni casi, delle azioni compiute (log)



UNIVERSITÀ DEGLI STUDI DI TRIESTE

Che tipo di accessi? Finalità chiara.

- Gestionali e carriere studenti (di solito a carico del fornitore, ma questo non scarica il titolare dalle incombenze GDPR o dal definire parametri di compliance NIS2)
- Accesso ad Identity Provider, punti nodali di autenticazione per minimizzare la diffusione delle password sui sistemi (Autenticazione delle risorse e portali WEB)

Che tipo di accessi? Finalità chiara.

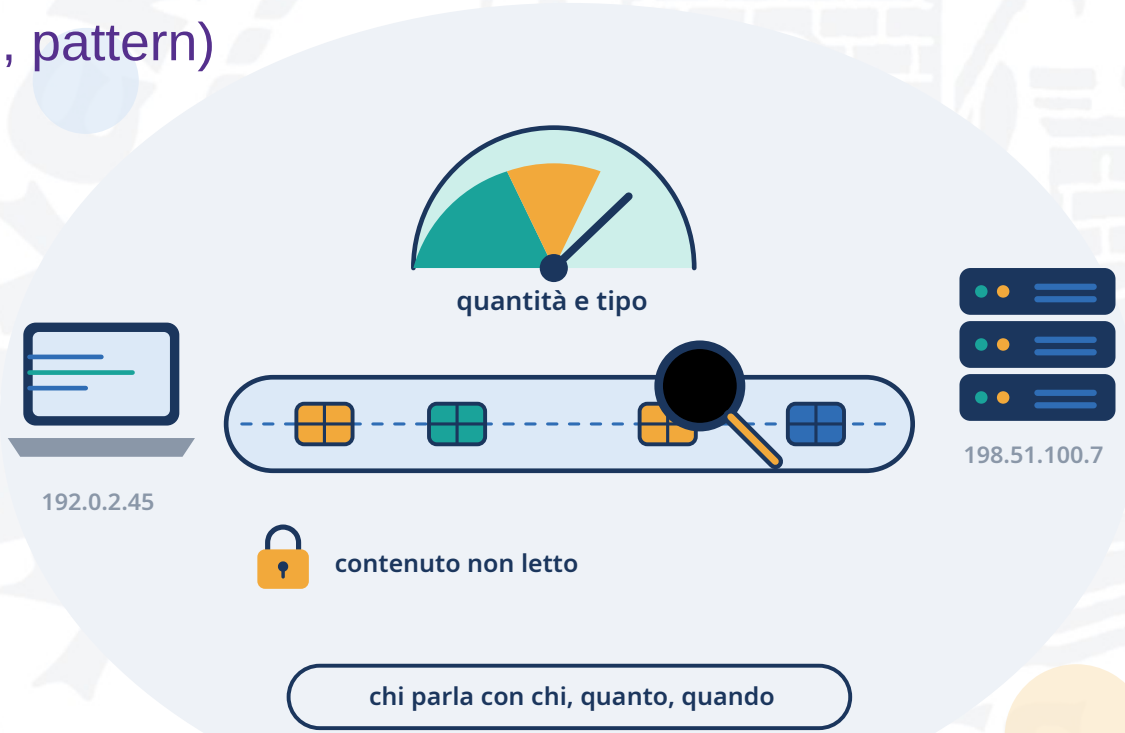
- VPN per accesso remoto e lavoro agile
  - Analisi malfunzionamenti
  - Analisi intrusioni
  - Autorità giudiziaria
  - ~~Sorveglianza dell'attività del lavoratore~~
- Accesso alla rete Wi-Fi e cablata (GARR eduroam 6 mesi)
  - Analisi malfunzionamenti (anche all'estero extra EU)
  - Analisi intrusioni (anche con l'estero extra EU)
  - Autorità giudiziaria
  - ~~Sorveglianza dell'attività del lavoratore~~

Che tipo di accessi? Finalità chiara.

- Posta elettronica (garante indica massimo 21 giorni)
  - Solo intestazioni, non contenuto
  - Analisi phishing e abusi
  - Analisi malfunzionamenti
  - Autorità giudiziaria
  - ~~Sorveglianza dell'attività del lavoratore~~
- Log dei server Web e dei portali
  - Analisi attività dell'utente
  - Analisi malfunzionamenti
  - Analisi abusi
  - ~~Sorveglianza dell'attività del lavoratore~~
- …

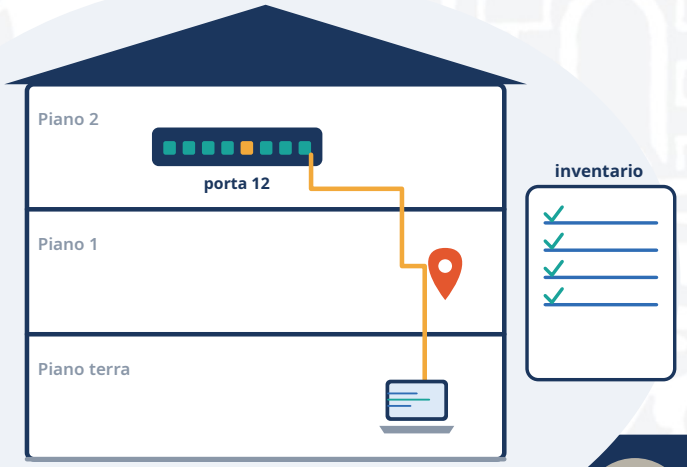
Accounting: Log meno scontati

- Log delle attività in rete fra indirizzi IP (netflow)
  - Quantità e tipologia di traffico (NO contenuto, pattern)
  - Analisi malfunzionamenti
  - Analisi intrusioni
  - Autorità giudiziaria
  - ~~Sorveglianza dell'attività del lavoratore~~



Accounting: Log meno scontati

- Corrispondenza IP – macchina (mac address) e localizzazione (quale porta di quale apparato su quale piano di che sede)
  - Prima e ultima attività rilevata
  - Tracciamnto degli asset e ausilio all'inventario (situazione reale, conservazione minima 5 anni ammortamento spese informatiche)
  - Risorse in ordine e ausilio alla dismissione asset datati e risorse corrispondenti
  - Analisi malfunzionamenti
  - Analisi intrusioni fisiche
  - Autorità giudiziaria
  - ~~Sorveglianza dell'attività del lavoratore~~



UNIVERSITÀ DEGLI STUDI DI TRIESTE

Elaborazione automatica: Log meno scontati

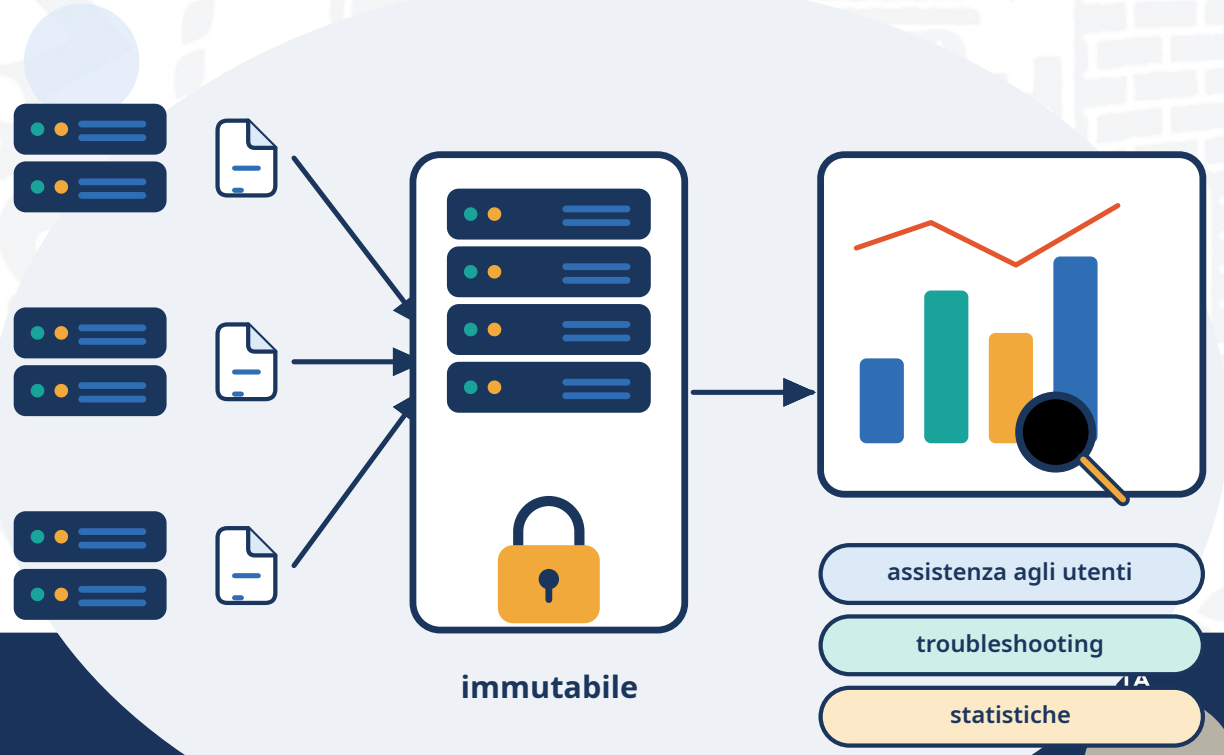


- Log di attività specifiche (DNS, metriche ad hoc)
- Di grande aiuto alla correlazione (SIEM)
- DNS dns.google.com → 8.8.8.8
  - Indicativo delle destinazioni di navigazione dell'utente e dei processi macchina
  - ~~Sorveglianza dell'attività del lavoratore~~
  - Analisi malfunzionamenti
  - Analisi intrusioni
  - 01-Oct-2026 10:37:42.183 client @0x7f3a84012c80 192.0.2.45#51432 (c2.example-malware.net): query: c2.example-malware.net IN A +E(0)K (192.0.2.53)



- Scoperta di macchine compromesse e silenti
- Insieme ad altri log permettono di fare prevenzione
- Prevenzione di:
  - Esfiltrazione
  - Attacchi rivolti alla rete e dati interni
  - Attacchi verso l’esterno
- Non prevenire vuol dire
  - Incidenti aperti con ACN (estremamente onerosi e possibilità assessment NIS2)
  - Danno reputazionale (si finisce sui media)

- Un **log server centralizzato** serve per rendere **immutabile** il log in caso di compromissione del singolo server
- Un **analizzatore di log** serve per correlazioni manuali e velocizzare attività di
  - Miglioramento proattivo del servizio
  - Assistenza agli utenti
  - Troubleshooting malfunzionamenti
  - Statistiche, evoluzione proattiva



- Raccolta parziale e analisi dei log
  - 300GB di dati raw al giorno
  - 12 vCPU
  - 64GB RAM
  - 10 TB disco



flusso continuo di log

CPU usage	27.85% of 12 CPUs
Memory usage	98.11% (62.79 GiB of 64.00 GiB)
SWAP usage	12.50% (8.00 GiB of 64.00 GiB)
Bootdisk size	54.20% (5.91 TiB of 10.91 TiB)

graylog Search Streams Alerts Dashboards Enterprise Security System 7,050 in 7,004 out

Search › Unsaved Search

Overview
User Activity
Host Activity
Network Activity
Anomalies

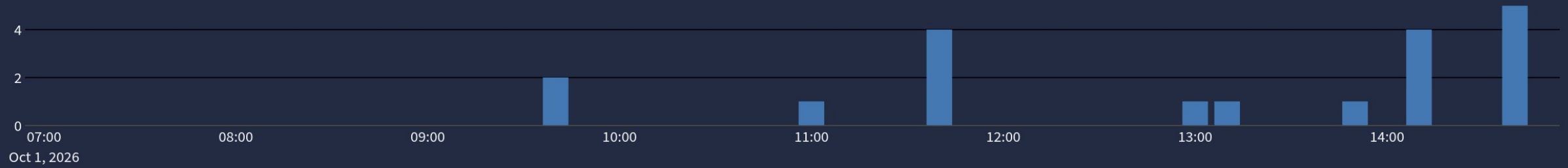
Query executed in 130ms at 2026-10-01 14:54:03 Total results: 19

From: **8 hours ago** Until: **Now** log base vari server Not updating

"user: [redacted]" Save Load Share

Filters

Message Count

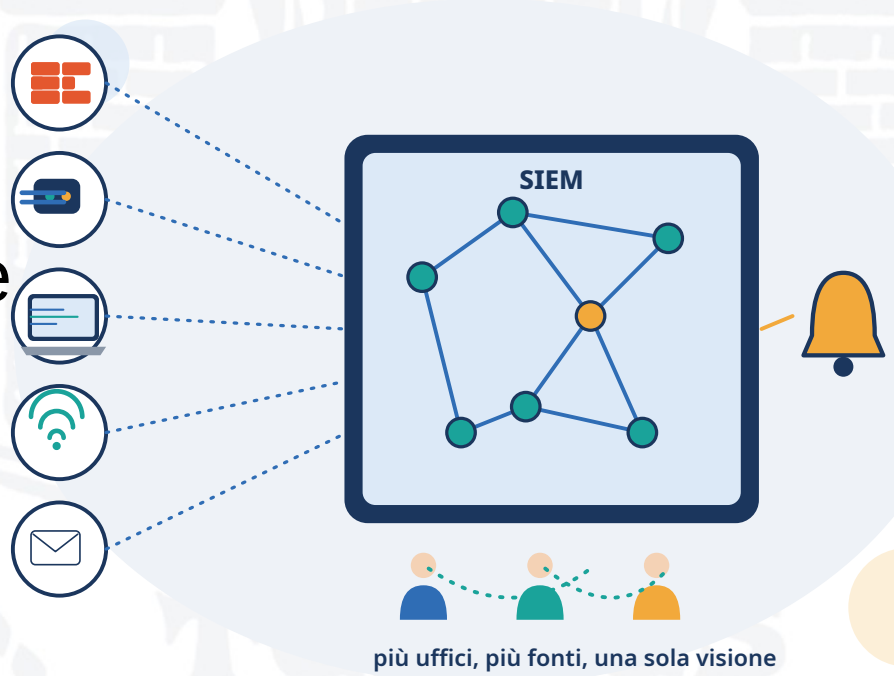


All Messages

timestamp	source	
2026-10-01 14:45:00.000	guard	guard eduvpn-radius[853]: 2026-10-01T14:45:00 INFO eduvpn-radius: start user=[redacted]units.it ip4=10.[redacted] ip6=2001:760:2e03:[redacted] profile=[redacted]-staticIP ok=True conn=EcA5[redacted]THE E
2026-10-01 14:44:56.000	guard	guard eduvpn-radius[853]: 2026-10-01T14:44:56 WARNING eduvpn-radius: disconnect per sessione sconosciuta user=[redacted].units.it conn=Lu8[redacted]GBX8
2026-10-01 14:44:56.000	guard	guard vpn-user-portal: CONNECT USER=[redacted].units.it PROFILE=[redacted]-staticIP PROTO=wireguard CONN=EcA5[redacted]IHEE/auYnhBDr[redacted]vlep/QrGU= IP4=10.[redacted] IP6=2001:760:2e03:[redacted] NODE=0 HOST=guard.units.it URL=http://localhost:41194
2026-10-01 14:44:56.000	guard	guard vpn-user-portal: DISCONNECT USER=[redacted].units.it PROFILE=[redacted]staticIP PROTO=wireguard CONN=Lu8Tp[redacted]UHLC/XGBNlv3[redacted]MXqCE0= BYTES_IN=23399888 BYTES_OUT=226336904 NODE=0 HOST=guard.units.it URL=http://localhost:41194
2026-10-01 14:43:18.000	guard	guard eduvpn-radius[853]: 2026-10-01T14:43:18 INFO eduvpn-radius: stop user=[redacted].units.it ip4=10.[redacted] ip6=2001:760:2e03:[redacted] profile=[redacted]staticIP ok=True conn=Lu8Tp[redacted]
2026-10-01 14:13:00.000	guard	guard eduvpn-radius[853]: 2026-10-01T14:13:00 INFO eduvpn-radius: start user=[redacted].units.it ip4=10.[redacted] ip6=2001:760:2e03:[redacted] profile=[redacted]staticIP ok=True conn=Lu8T[redacted]

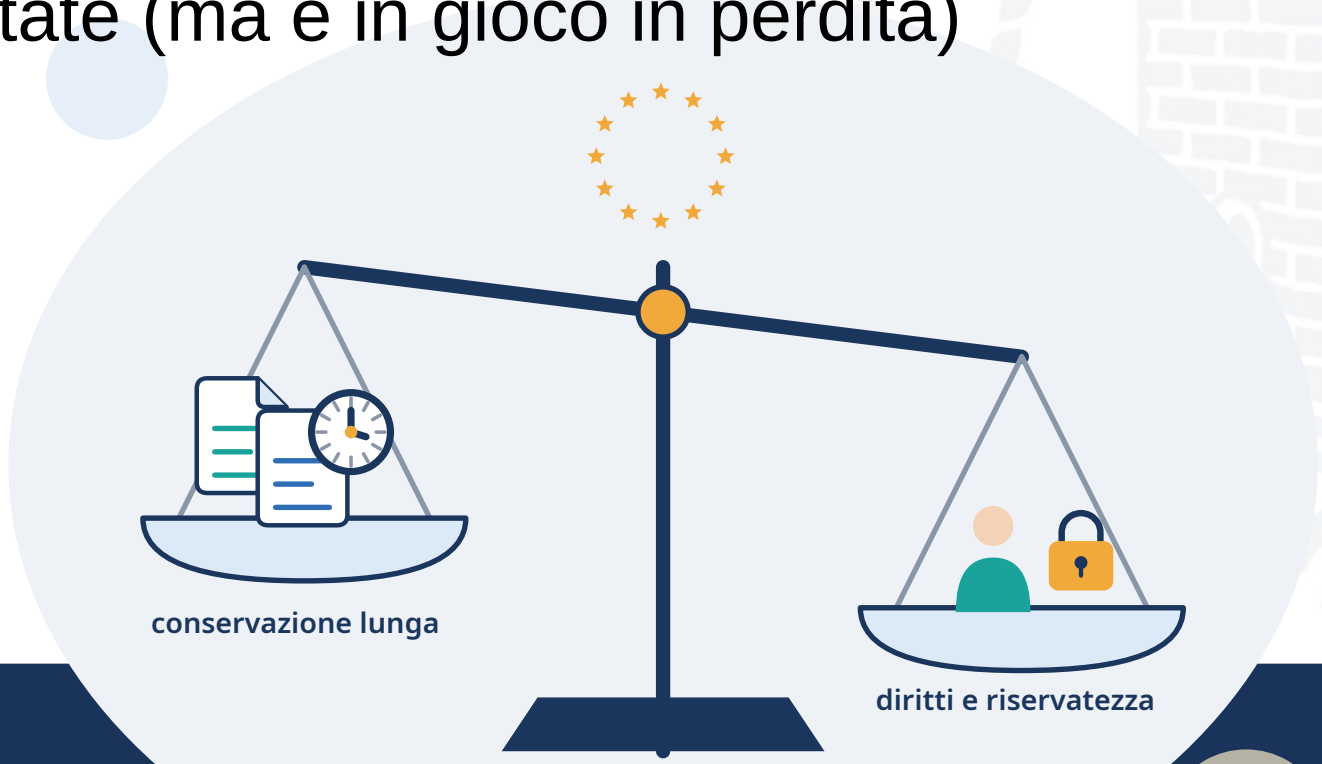
SIEM: Log meno scontati

- Un SIEM (Security Information and Event Management) raccoglie, aggrega e analizza in tempo reale i log e gli eventi provenienti da **tutta** l'infrastruttura IT di un'organizzazione
- Un SIEM con 4 sorgenti è del tutto inutile
- In realtà medie e grandi è necessario la **collaborazione fra uffici** per far confluire queste informazioni
- ~~Sorveglianza dell'attività del lavoratore~~



- Minacce cibernetiche sempre più:
  - **Frequenti**: in 2 anni 2 grosse università. “Non se, ma quando capita.”
  - **A tempo**: accesso iniziale riferibile a più di 10 mesi prima: rivedere tempi massimi di conservazione dei log (GDPR)
  - **Nascoste**: movimenti laterali oculati e che lasciano pochissime o nessuna traccia
- Combattere questo vuol dire
  - Quantità importanti di informazioni non anonimizzate da collezionare, conservare, analizzare
    - Costi maggiori in termini di hardware
    - Nuovi sistemi di analisi da mettere in piedi (costi in risorse umane)

- La conservazione a lungo termine **va giustificata** insieme al RPD/DPO per quanto riguarda la compliance al GDPR
- Facile forse solo a valle di compromissioni long-standing documentate (ma è in gioco in perdita)

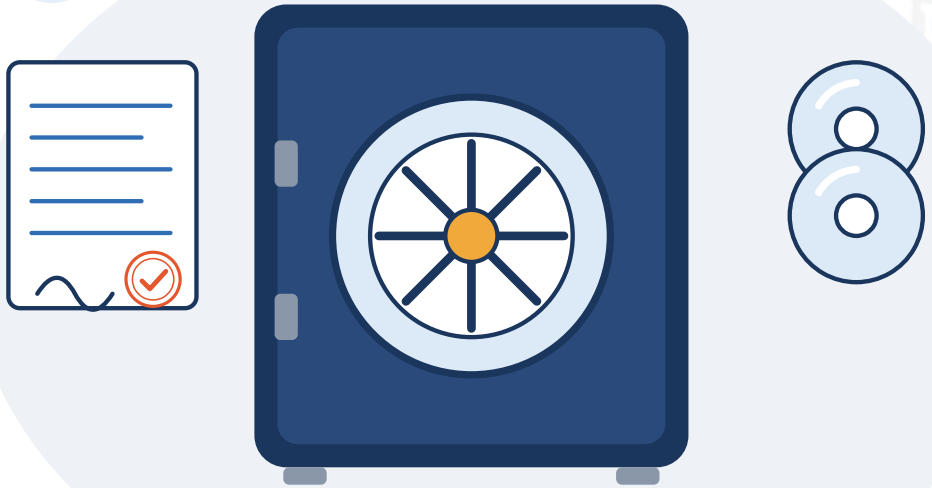


- L’IT si attende indicazioni (scritte) dal management in quanto
  - cosa rendere immutabile
  - cosa mandare in conservazione sostitutiva
  - per quanto tempo

  sono scelte dettate da esigenze di ordinaria difesa in tribunale, ma non hanno alcuna rilevanza informatica.
- Importanti anche le indicazioni sulla retention in seguito a estrazione (altrimenti vale la retention normale anche in caso di uso per difesa in tribunale)

UNIVERSITÀ DEGLI STUDI DI TRIESTE

- Per alcuni log è necessario mettere in piedi dei meccanismi di non ripudio / immutablità
- Qualcuno usa i dispositivi WORM (write once read many)? DVD-R, BlueRay, dischi magneto-ottici?



Accountability legale dell’amministratore di sistema

- In assenza di dispositivi finalizzati all’archiviazione con garanzia di integrità e immutabilità, anni fa ho messo su una soluzione “fai da te”

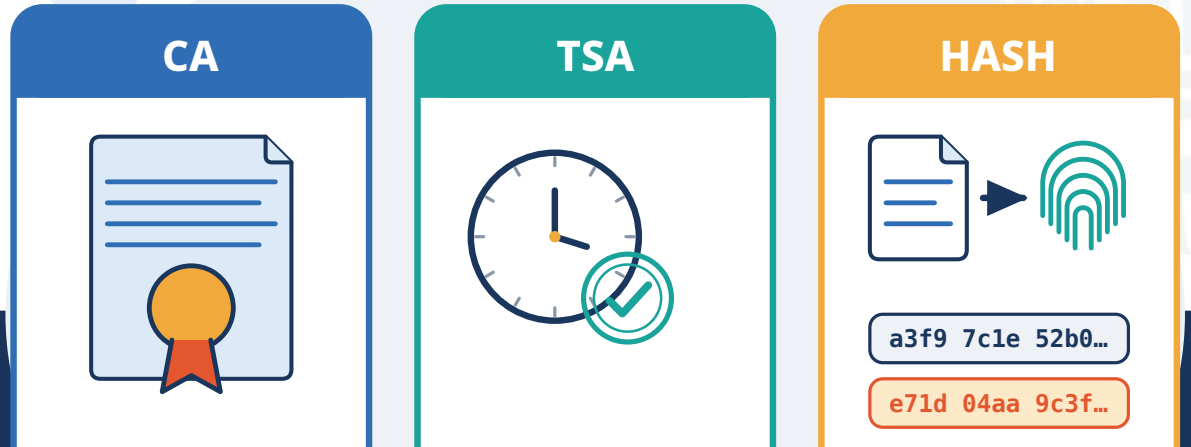


Non vale come prova in tribunale perché non usa CA e TSA accreditate AgID che offrono questi servizi a pagamento e non a singoli amministratori di sistema



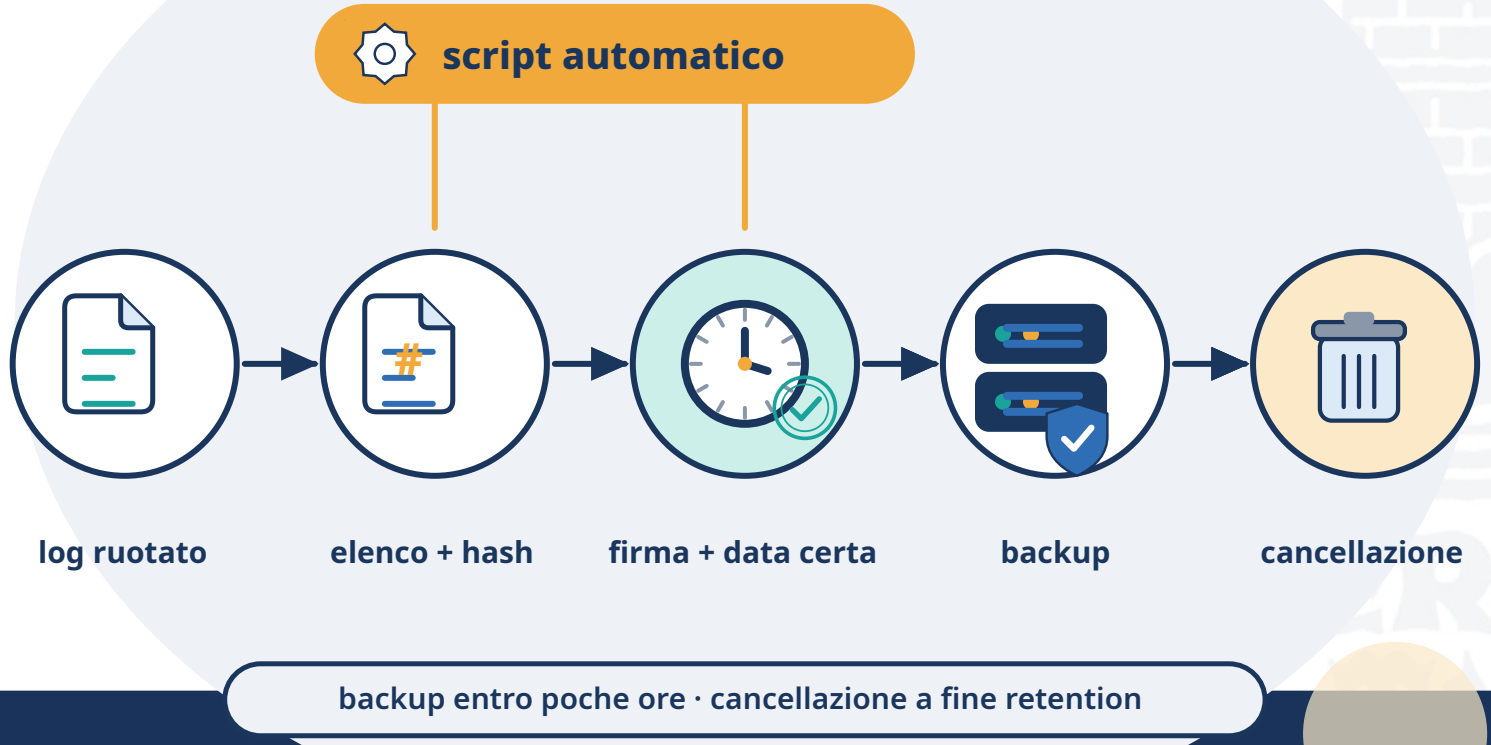
Si basa su asserzioni di terzi la cui collusione (non c’è e) va comunque dimostrata. Potrebbe spostare l’onere della prova. Costo quasi zero

- **CA: certification authority.** Rilascia certificati digitali, firme digitali
- **TSA: timestamp authority.** Rilascia marche temporali per definire la data certa
- **HASH:** è una funzione matematica che, preso in ingresso un dato di qualsiasi dimensione, calcola una stringa di lunghezza fissa, detta hash, digest o impronta. Una piccola modifica dell'input produce normalmente un hash completamente diverso.



Cosa succede ai miei log

- Log radius: accesso al Wi-Fi, rete via cavo autenticata e VPN
- Vengono ruotati dal sistema una volta a giorno sempre alla stessa ora per ogni server



UNIVERSITÀ DEGLI STUDI DI TRIESTE

Cosa succede ai miei log

- Alla procedura di rotazione ho agganciato uno script (programma scritto da me) che:
  - Crea un file di testo con il nome dei file di log affiancati dal loro hash sha-256
  - Contatta una timestamp authority gratuita, ottiene la firma del file con la data certa e lo salva in un file con lo stesso nome ma estensione diversa
- I file così ottenuti, insieme ai log, vengono backupati dal server di backup entro qualche ora
- I log vengono automaticamente cancellati dopo il periodo di retention

UNIVERSITÀ DEGLI STUDI DI TRIESTE

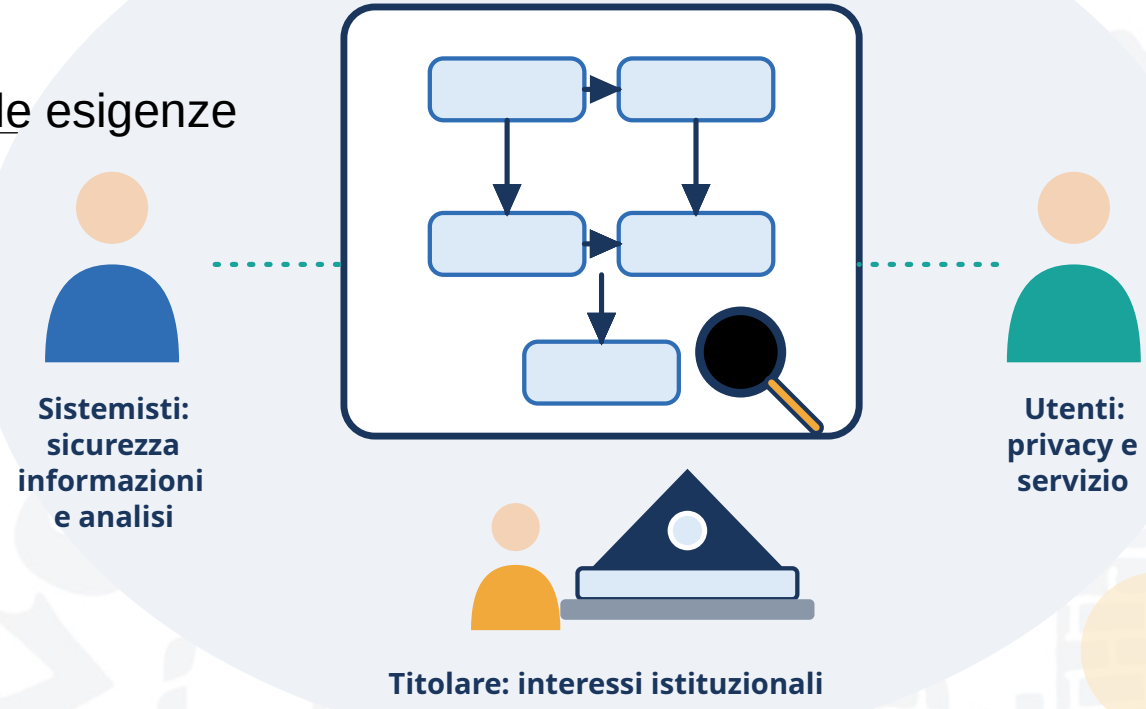
Risultato



- File in uso difficilmente modificabile
- Rotazione, timestamp e firma quasi contestuali
- Estrema difficoltà nella alterazione dei dati (tampering) anche intenzionale

- Speranza che queste caratteristiche scarichino la responsabilità soggettiva in mancanza di altri elementi

Far convergere le esigenze



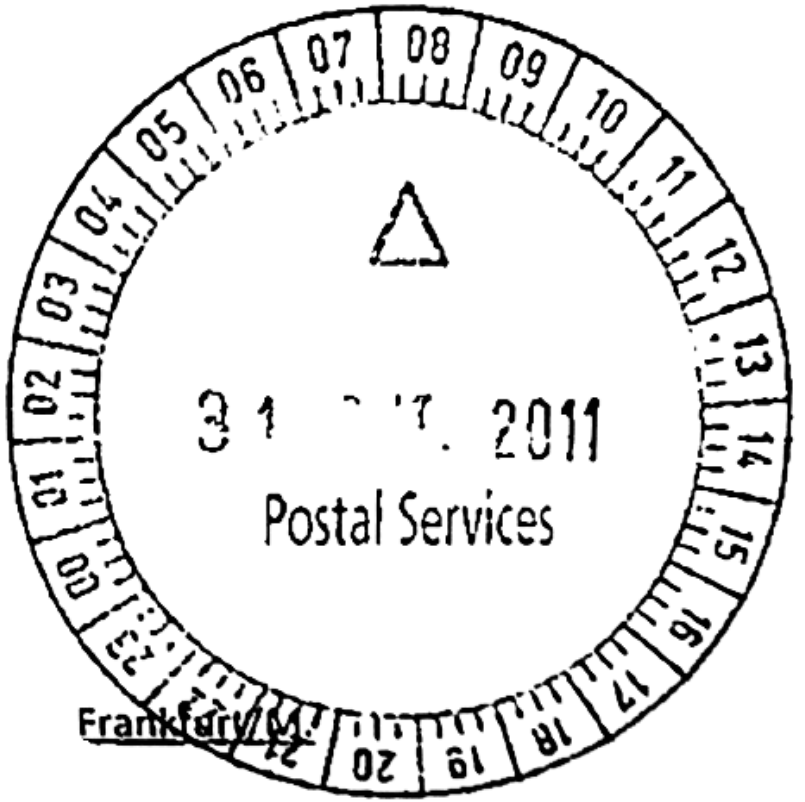
- Analizzare a fondo le procedure in essere
- Discernere sulle motivazioni, sugli interessi e sulla reale utilità per i vari soggetti coinvolti
  - **Utenti**: privatezza e servizio
  - **Titolare** (e altri uffici amministrativi): interessi istituzionali
  - **Amministratori di sistema**: sicurezza delle informazioni, analisi e prevenzione
- Analizzare bene tutti i flussi dei dati

Registro del trattamento: un punto di partenza

- Un registro del trattamento ordinato può venirci in aiuto fra le altre cose per
  - Individuazione dei diversi tipi di trattamento
  - Individuazione di quali dati vengono trattati (natura dei dati)
  - Individuazione dell'utenza interessata
  - Individuazione di trattamenti transnazionali e extra UE
  - ...

UNIVERSITÀ DEGLI STUDI DI TRIESTE

All sent



CC-BY-SA Jan Schejbal