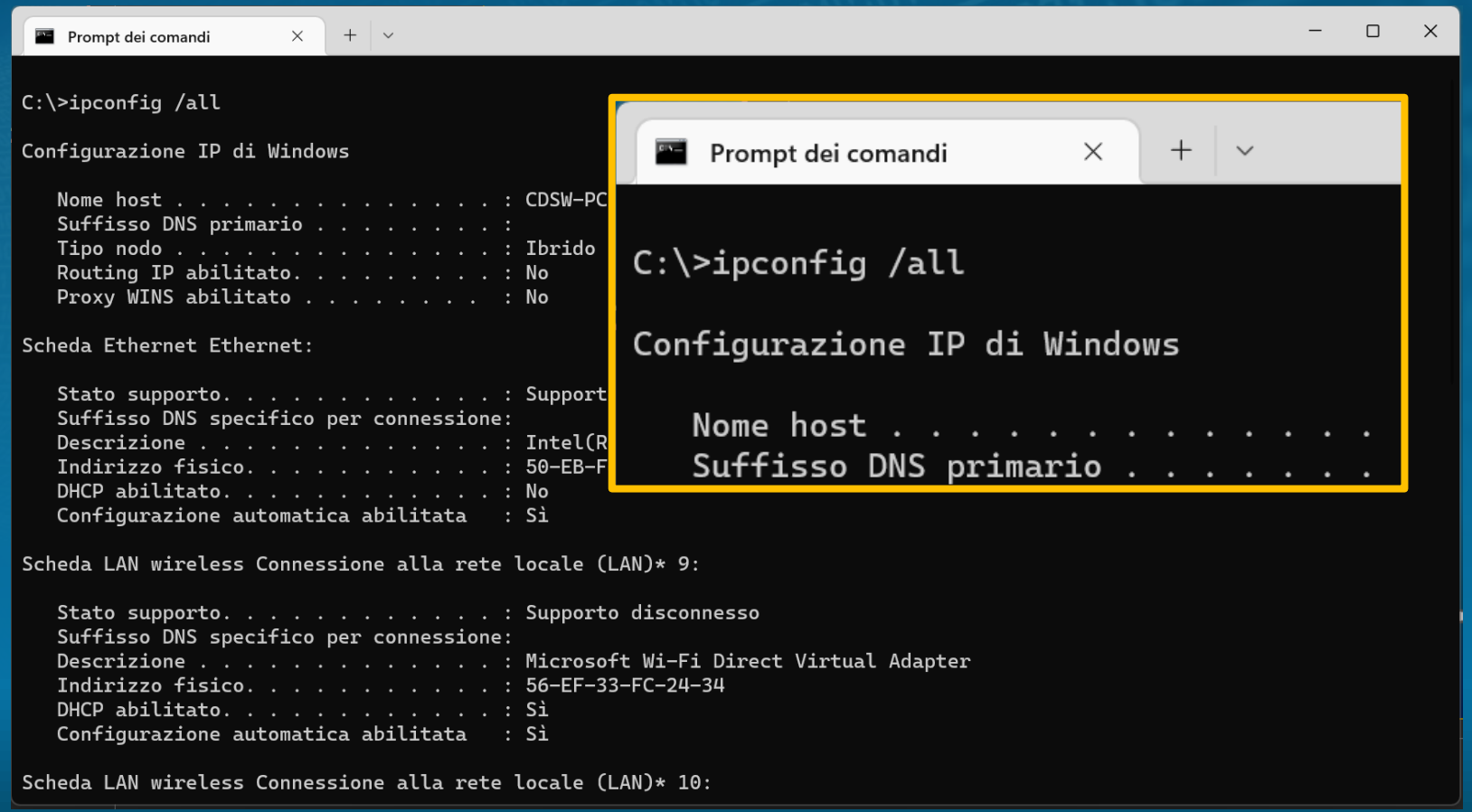
# CYBER SECURITY

Lezione 06 – Il monitoraggio

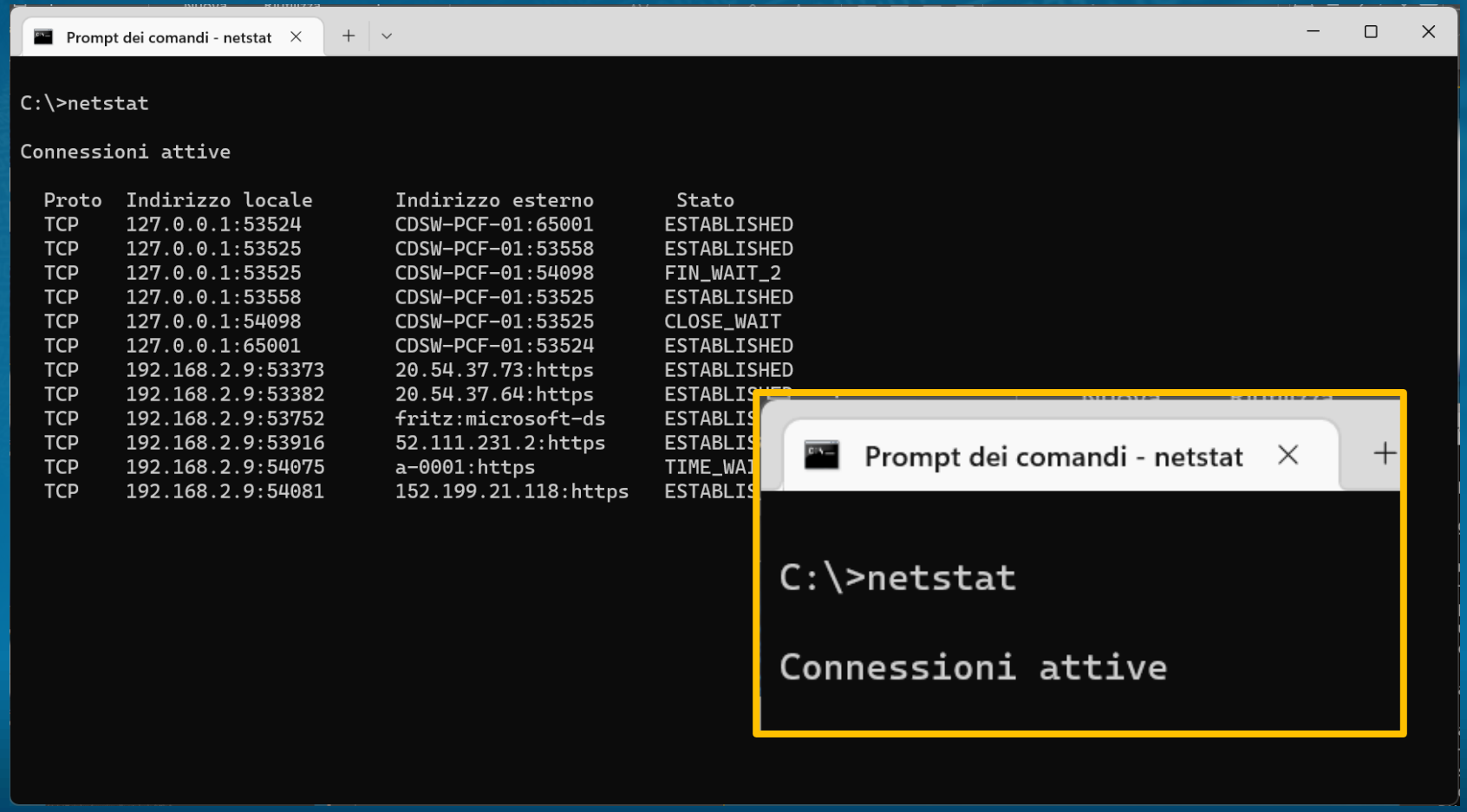
# Il Monitoraggio : le connessioni

- Controllare lo stato delle connessioni con la console



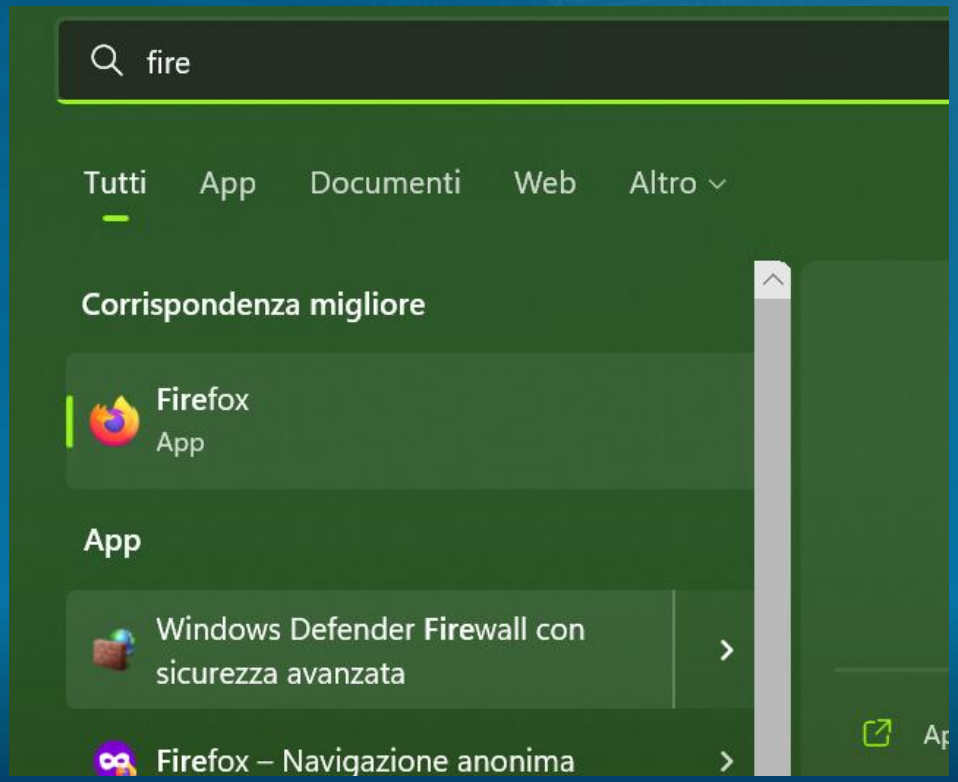
# Il Monitoraggio : le connessioni

- Controllare lo stato delle connessioni con la console
- Verificare con whois e dnslookup chi sono gli indirizzi presenti in lista
- Salvare i dati a 'macchina pulita'
- In caso di attacco confrontare i dati correnti con quelli salvati

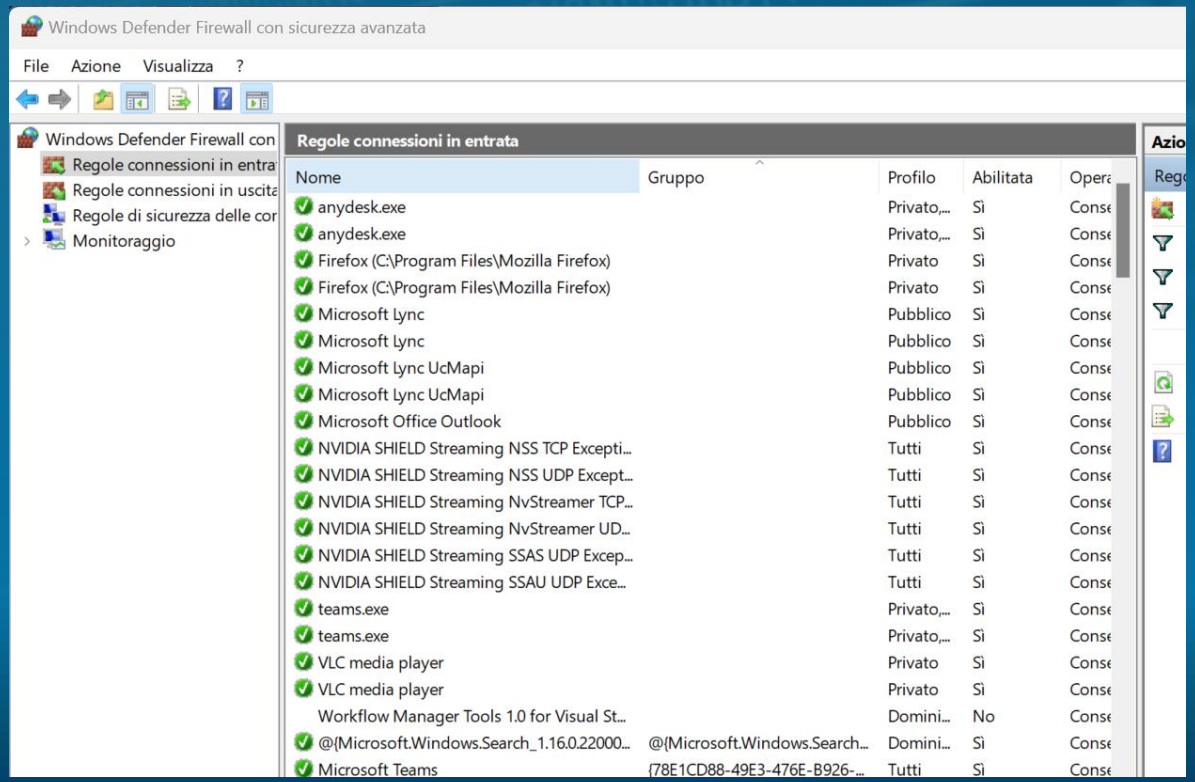


# Il Monitoraggio : il Firewall

- Aprire il firewall in modalita' Avanzata

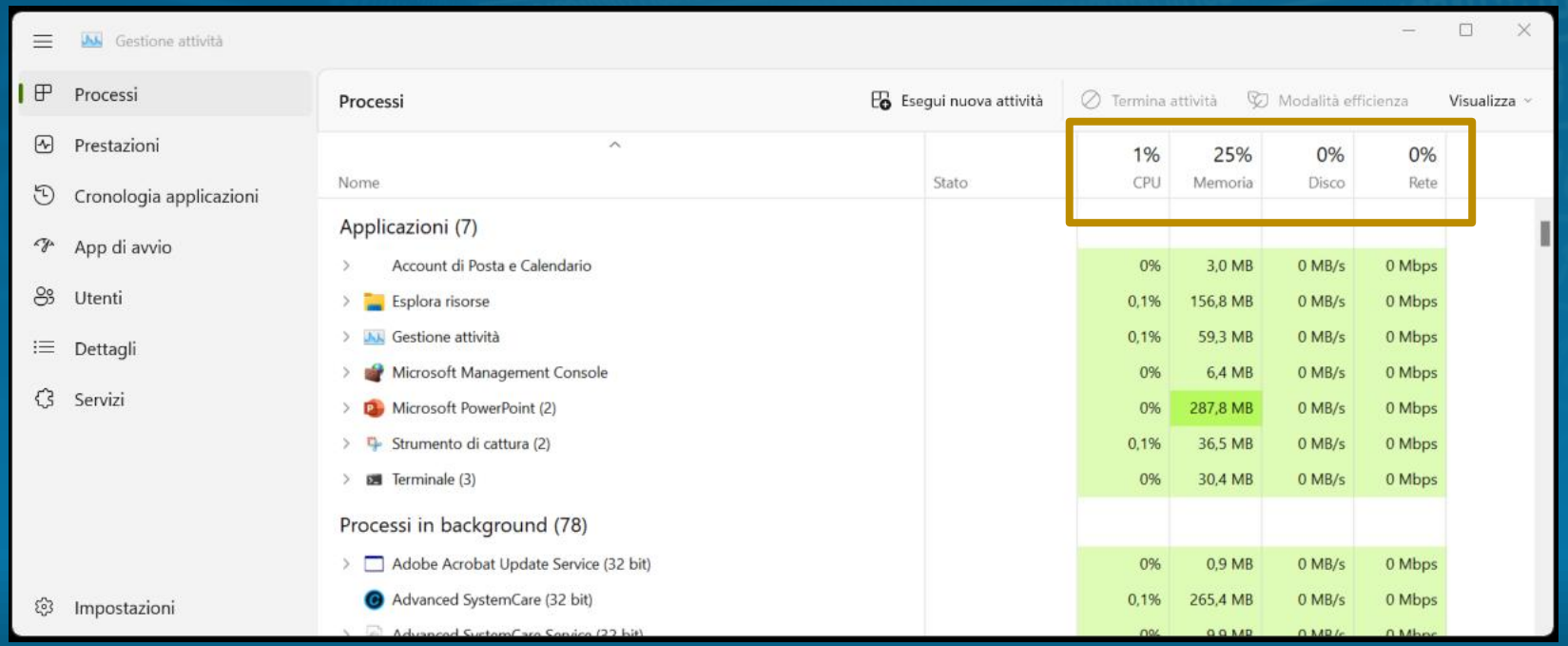



- Rimuovere tutte le regole superflue (Ripristino per reset)



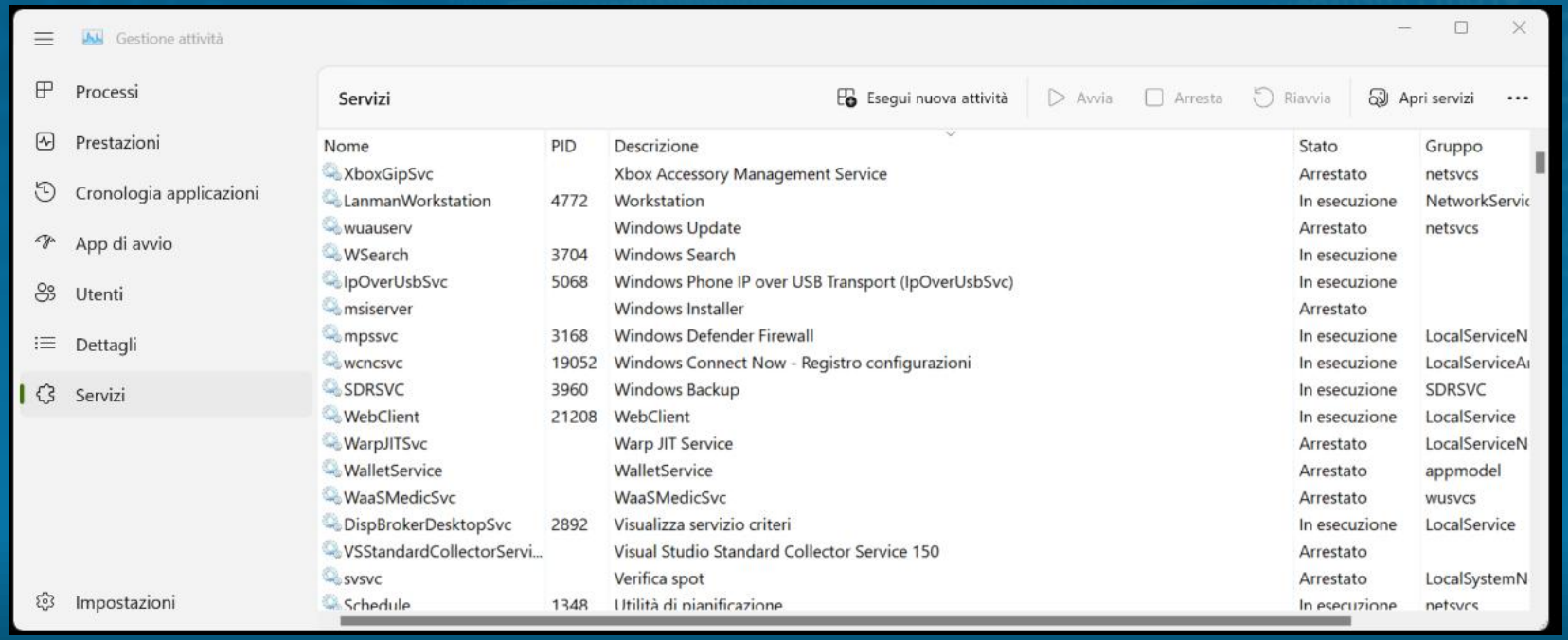
# Il Monitoraggio : I Servizi e i Processi

- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto



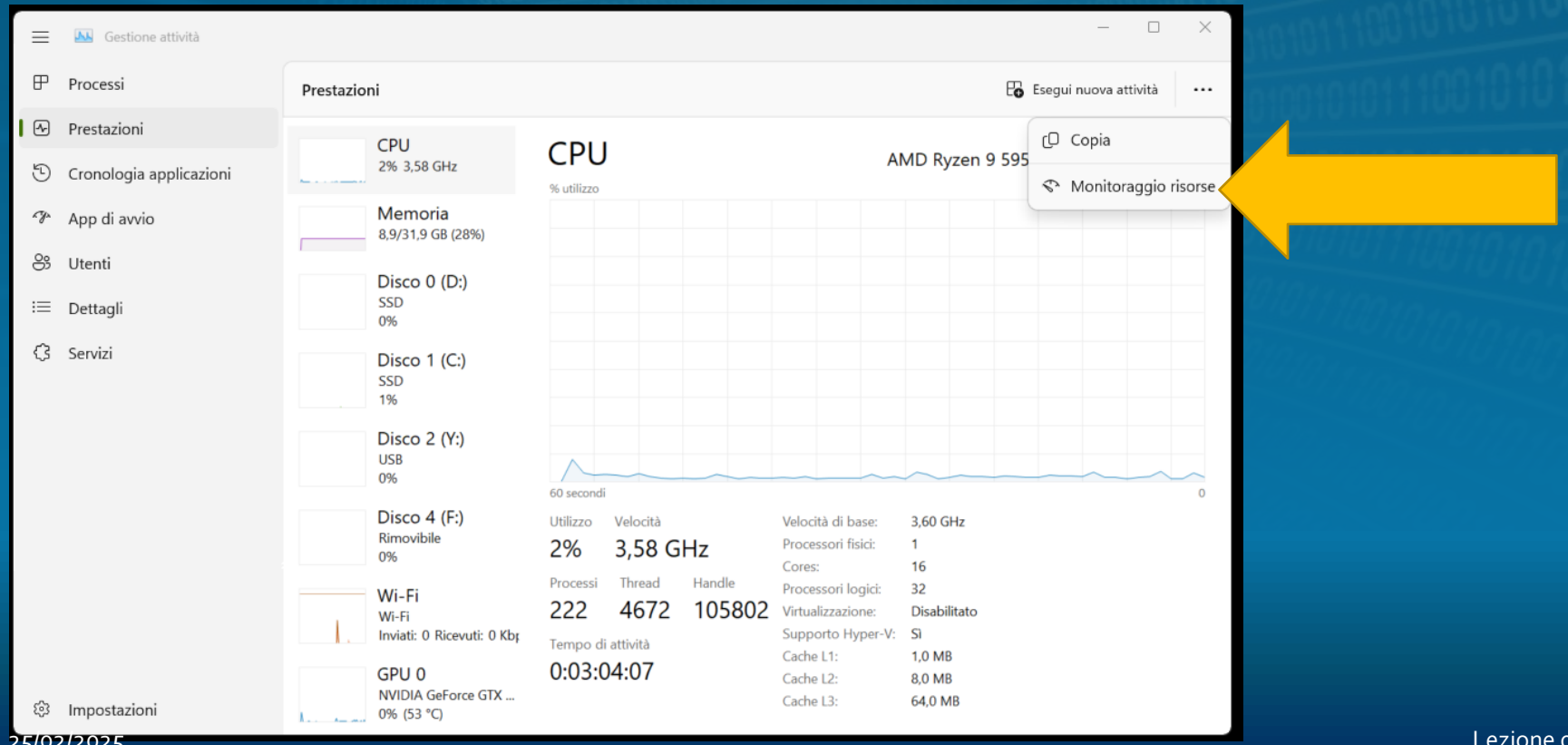
# Il Monitoraggio : I Servizi e i Processi

- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto



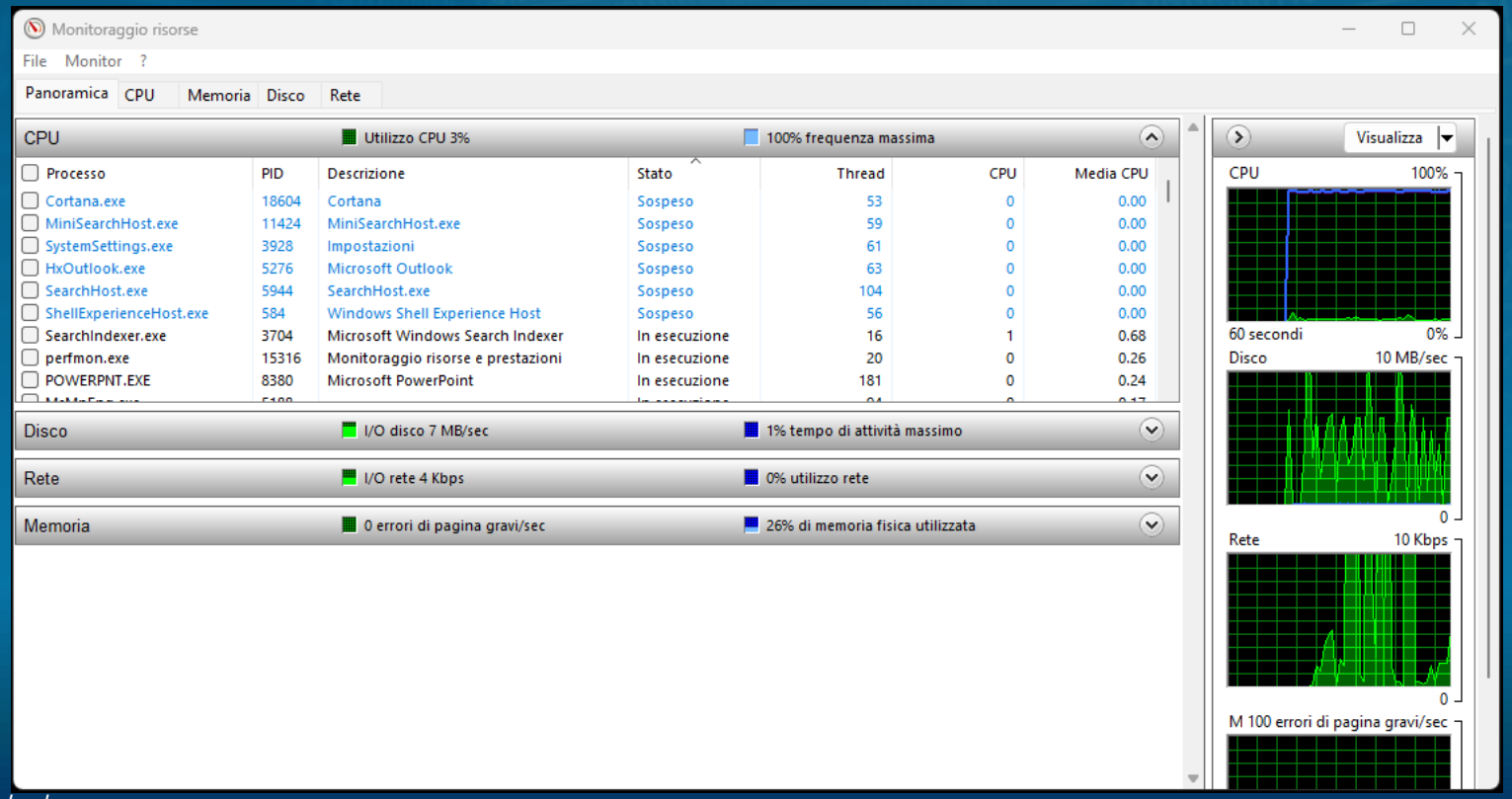
# Il Monitoraggio : Le Prestazioni

- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto



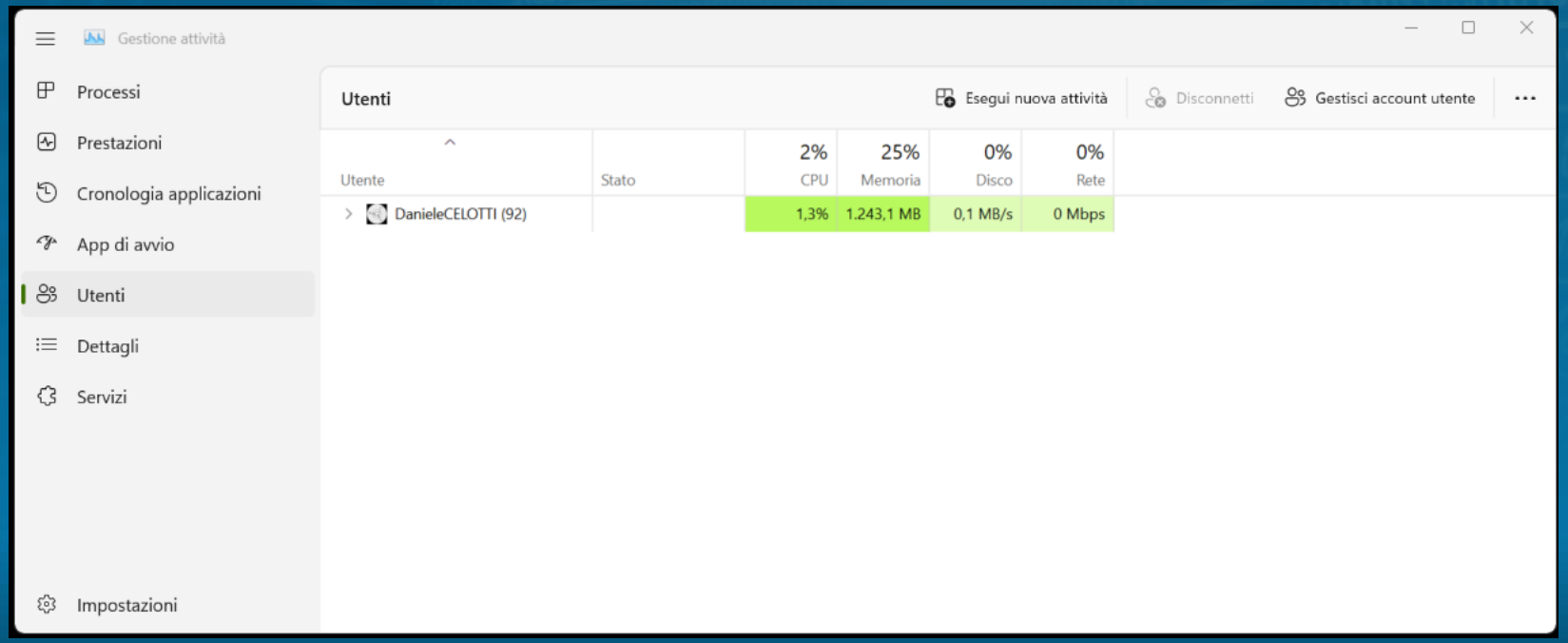
# Il Monitoraggio : Le Prestazioni

- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto



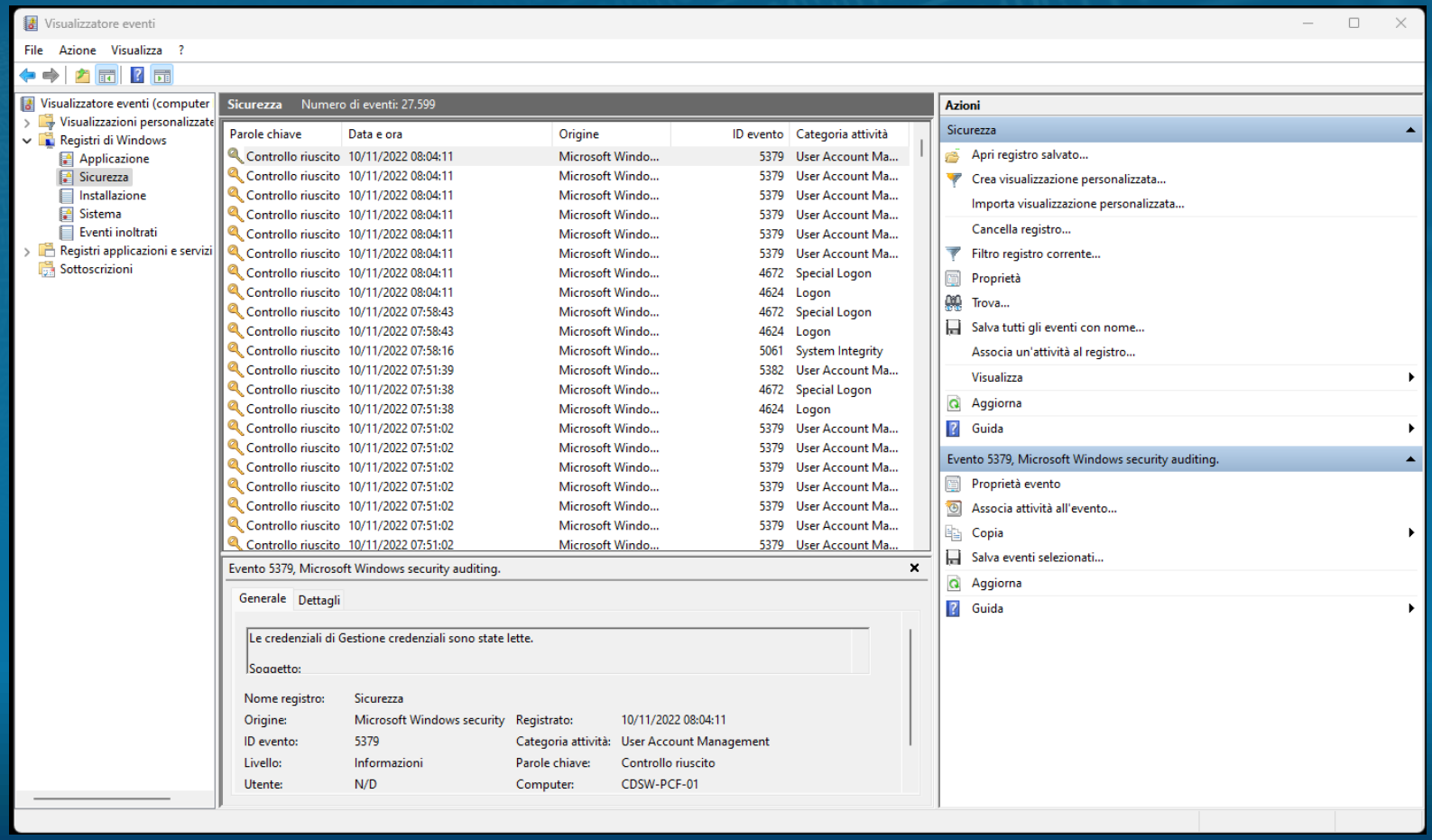
# Il Monitoraggio : Gli Utenti attivi

- Osservare se ci sono utenti indesiderati



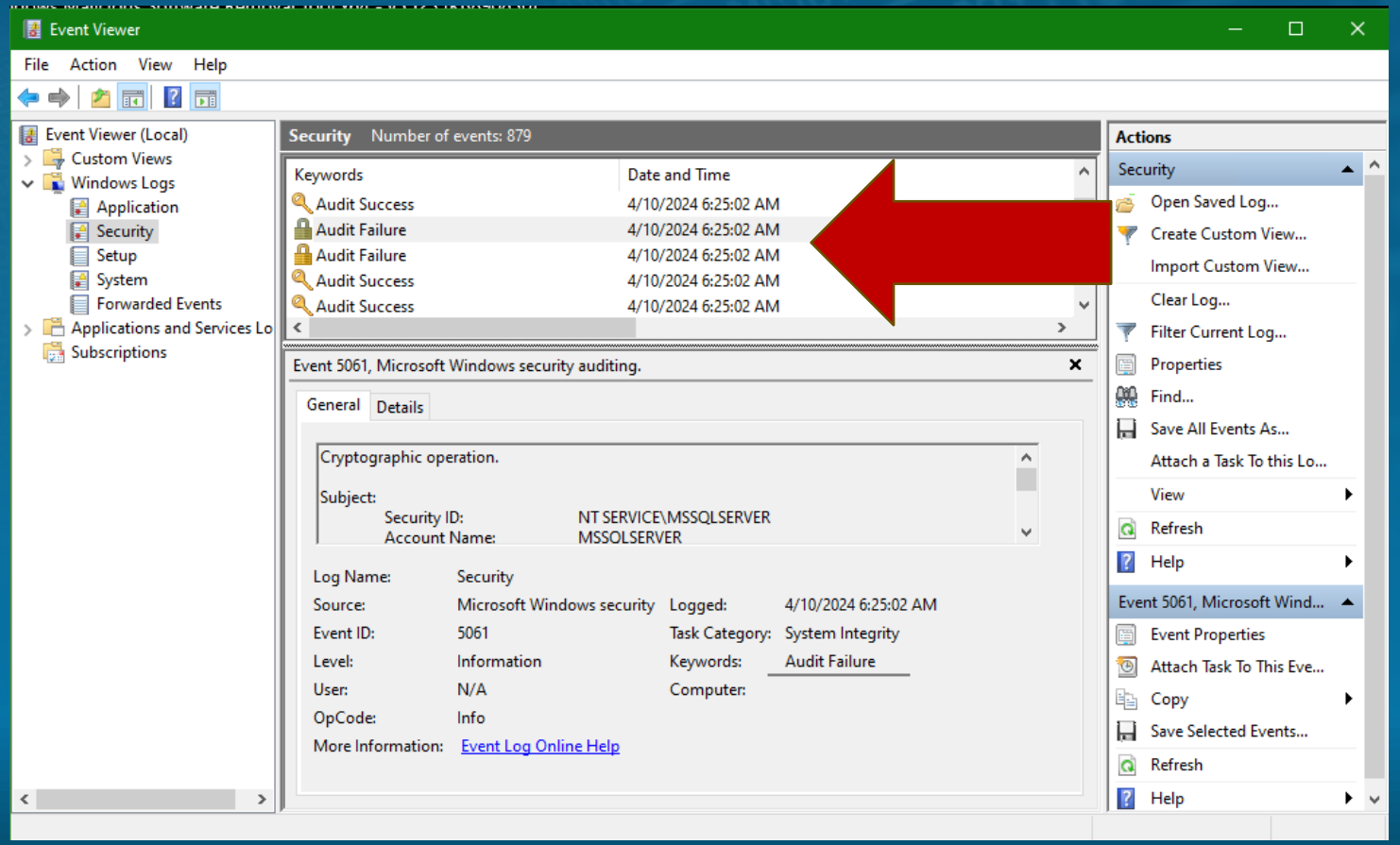
# Il Monitoraggio : Visualizzare gli Eventi

- Creare un'immagine dello stato iniziale e pulito del dispositivo per confrontarla in caso di sospetto



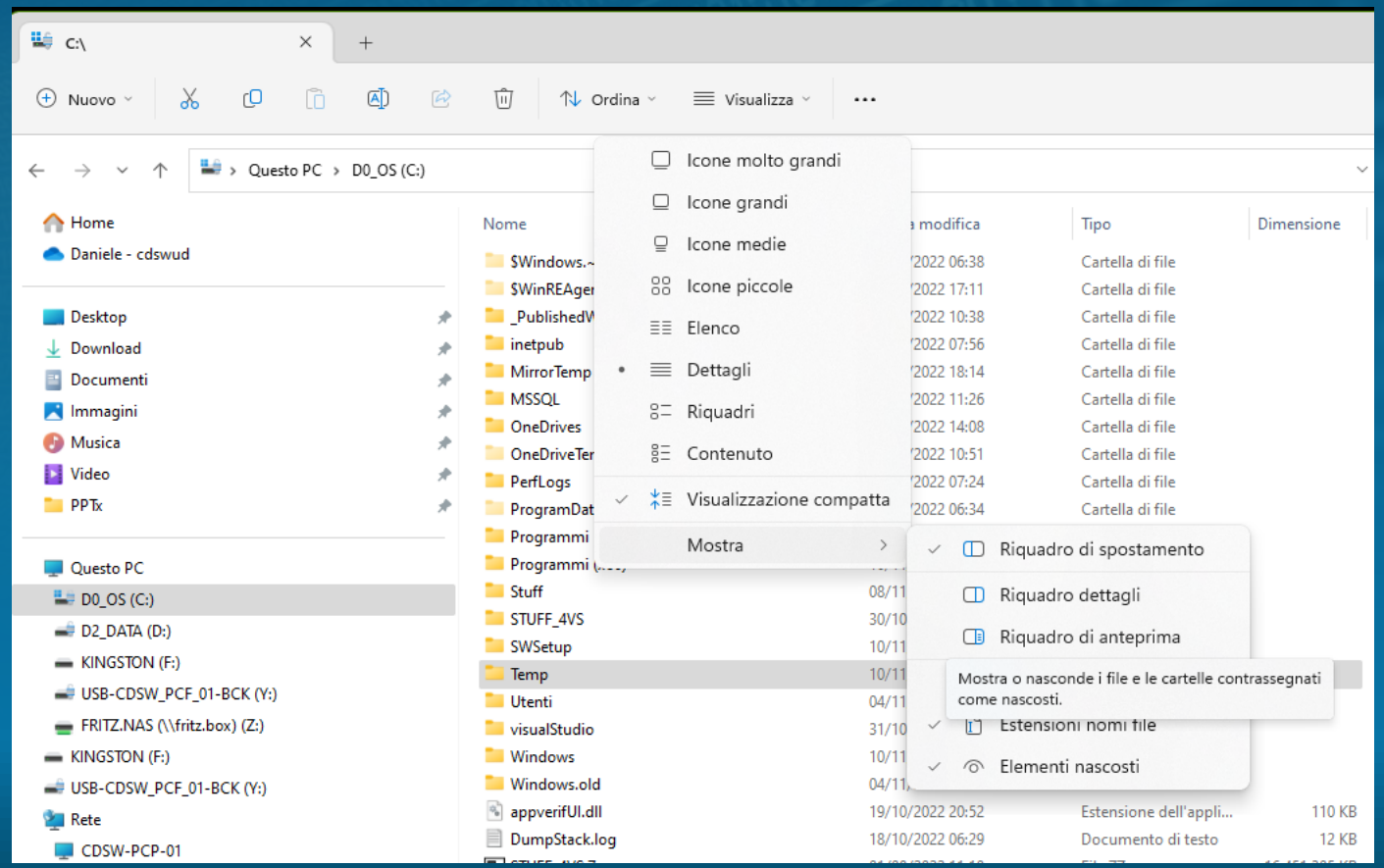
# Gli Eventi di sistema

Analisi degli eventi per scoprire  le intrusioni



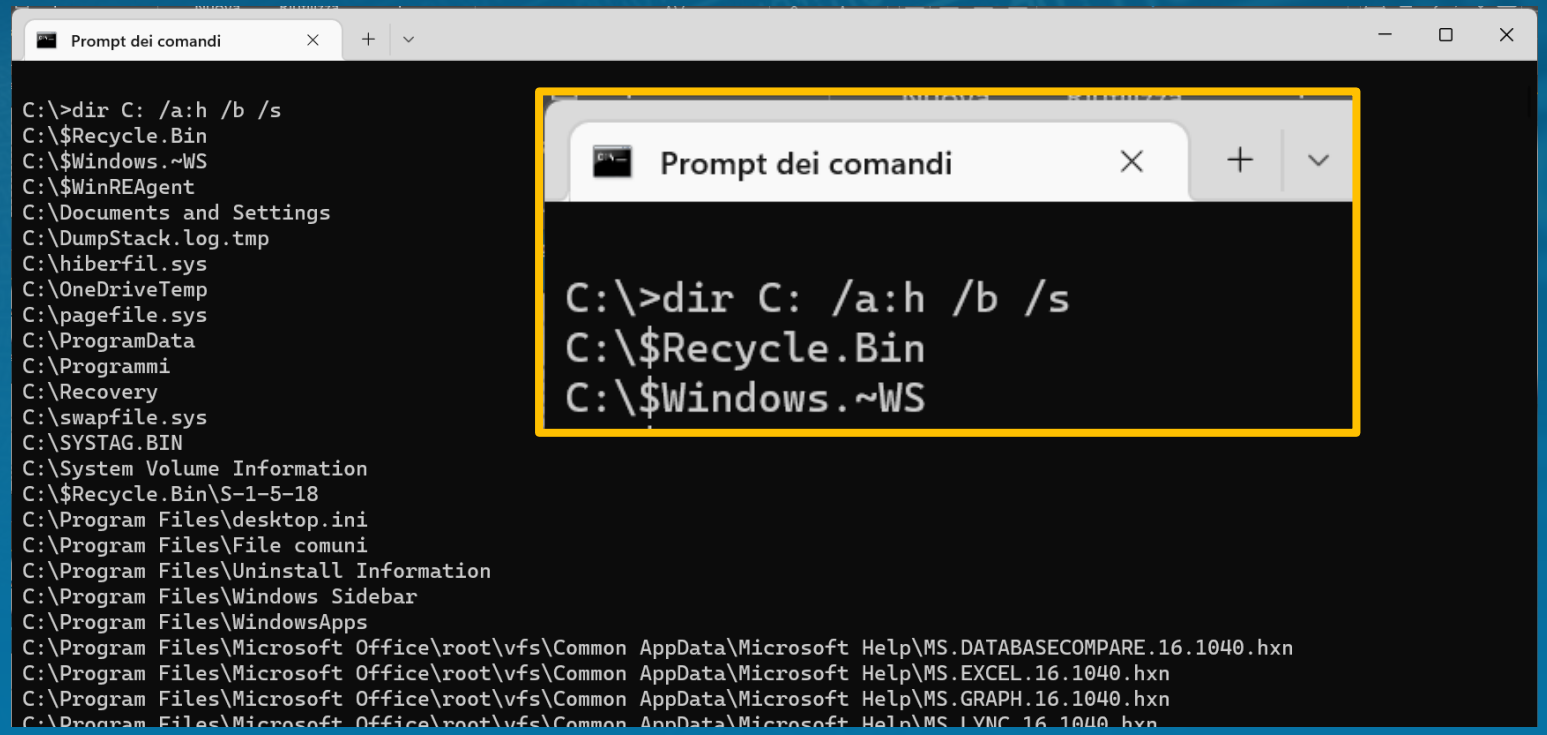
# Il Monitoraggio : Le Cartelle Nascoste

- Analizzare le cartelle nascoste o sospette per rilevare intrusioni ed attivita' indesiderate



# Il Monitoraggio : Le Cartelle Nascoste

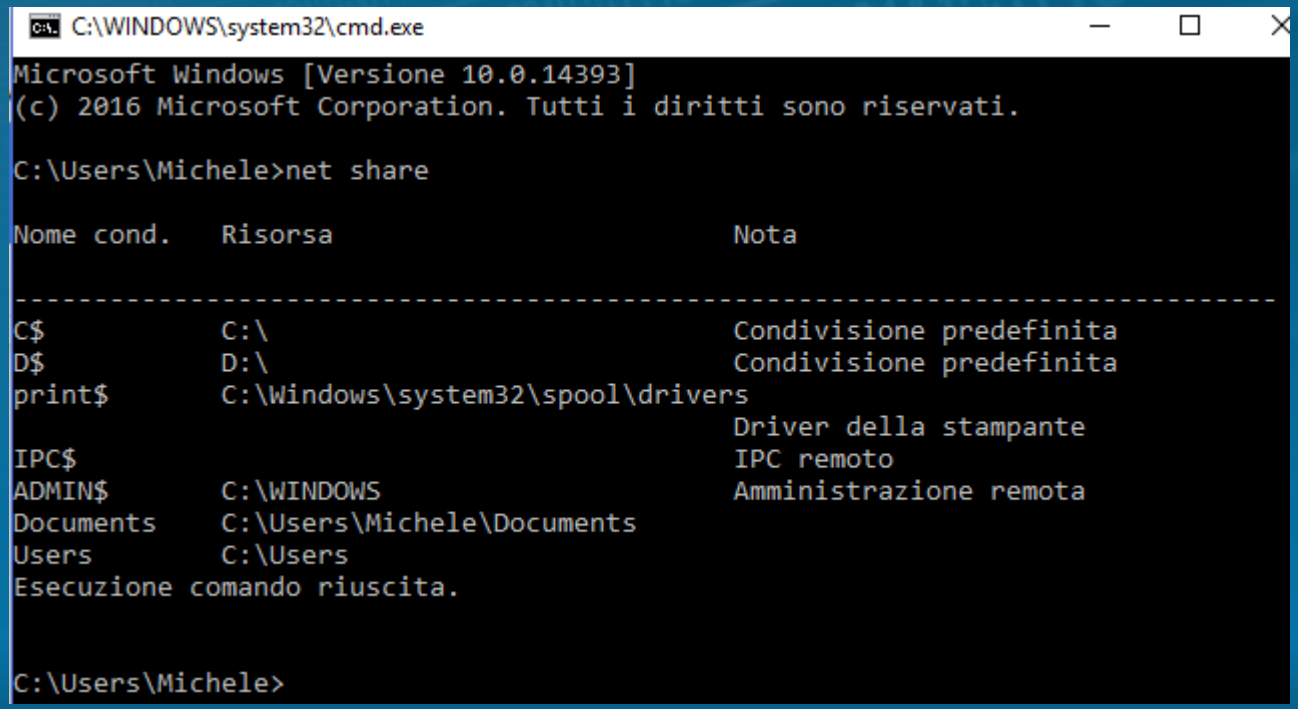
- Analizzare le cartelle nascoste o sospette per rilevare intrusioni ed attivita' indesiderate




How to Show Hidden Files Windows 10 (CMD + 4 Ways) (minitool.com)

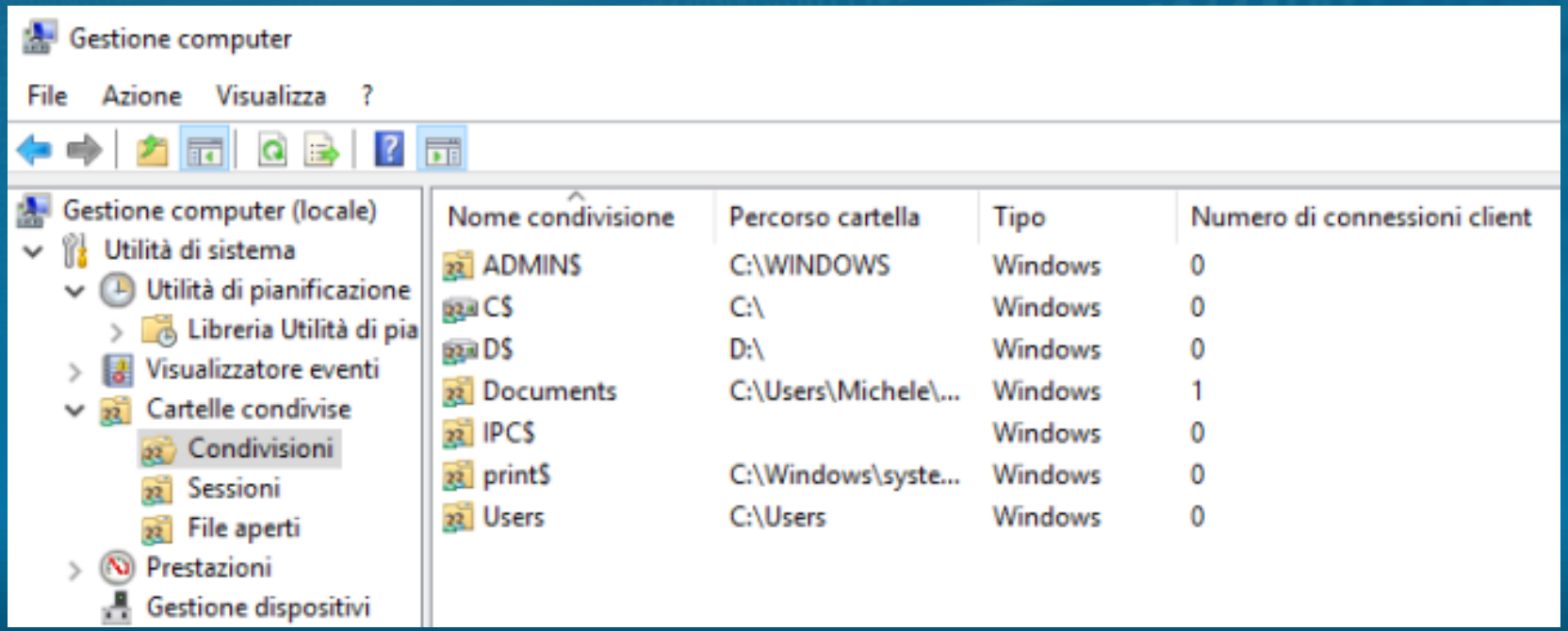
# CARTELLE CONDIVISE

- Premere Windows+R quindi digitare \\localhost
- Windows+R, cmd poi net share



# Cartelle condivise

- Premere Windows+R quindi digitare \\localhost
- Windows+R, cmd poi net share
- Gestione computer



# E NATURALMENTE…

- **Controllo Sistemi di Sicurezza**
  - Sicurezza Fisica
  - Antivirus ed Antispyware attivo, funzionante ed aggiornato
  - Servizio di aggiornamento del Sistema Operativo acceso e funzionante
  - Intrusion Detection System (per chi ce l'ha)
  - Restore da Backup
  - Firewall non compromesso
  - Regole delle password e dei gruppi

# In sintesi…

- **Backup dei dati**
  - Eseguire backup regolari di tutti i file di dati.
  - **Testare** il ripristino dei file di dati del client per garantire che i file di backup funzionino.
  - Assicurati che almeno una copia dei dati sia archiviata in un luogo sicuro fuori sede.
  - Rivedi periodicamente i tuoi requisiti di backup.

# In sintesi…

**Sicurezza fisica**

- Assicurati che i tuoi computer si trovino in aree non facilmente accessibili agli estranei.
- Assicurati che tu e il tuo personale siate responsabili della chiusura di porte e finestre.
- Verifica se i tuoi computer desktop e laptop sono dotati di dispositivi antifurto.
- Verifica se i tuoi server di rete sono fisicamente protetti in un'area separata.
- Assicurati di avere un inventario accurato di tutte le apparecchiature informatiche e dei software archiviati fuori sede.
- Implementa una politica di "svuotamento scrivania" per garantire che il tuo personale protegga i file sensibili e riservati quando non ci sta lavorando.

# In sintesi…

**Protezione dai virus**

- Controlla se il software antivirus è installato su tutti i tuoi computer.
- Verificare se il software antivirus è stato configurato per verificare la presenza di virus su tutti i supporti (e-mail, siti Web, file scaricati).
- Verificare se è in atto una procedura per l'aggiornamento automatico del software antivirus.
- Verifica se gli utenti sanno cosa fare quando vengono infettati da un virus informatico.
- Assicurati che tu e il tuo staff apriate solo gli allegati che si aspettano.

# In sintesi…

**Ripristino di emergenza**

- Avere un piano di continuità scritto in atto in caso di un grave disastro (come un incendio).
- Controlla per quanto tempo la tua pratica potrebbe funzionare senza computer, server o accesso alla rete.
- Verifica se la tua sede centrale fornisce assistenza per il ripristino di emergenza.
- Assicurati di avere almeno una copia dei dati del client e del software applicativo archiviata in un luogo sicuro fuori sede.
- Assicurati di avere un inventario aggiornato delle apparecchiature informatiche, del software e dei file client critici.

# In sintesi…

**Firewall**

- Controlla se su tutti i tuoi computer è installato un software firewall.
- Assicurati che il software firewall sia stato configurato per proteggere le informazioni richieste sui tuoi computer.
- Verifica se nella tua rete è installato un firewall hardware.
- Controlla se hai firewall installati in ogni punto in cui i tuoi sistemi informatici sono collegati ad altre reti.

# In sintesi…

## Gestione delle password

- Richiedi password per l'accesso a tutti i computer.
- Scegli password "forti".
- Cambia le password regolarmente.
- Assicurati che le password non siano scritte o condivise.
- Impedisci agli utenti di scegliere password che sono state utilizzate solo poco tempo fa.
- Disattivare gli account per i dipendenti licenziati in modo tempestivo.

# In sintesi…

**Varie**

- Non archiviare informazioni sensibili su unità USB
- Cancella frequentemente i dati privati dai browser Web.
- Assicurati che il tuo sistema operativo sia aggiornato.
- Utilizzare uno screen saver protetto da password o "bloccare" lo schermo.