

Gestione dei Log di Sicurezza con il Visualizzatore Eventi di Windows

UNA GUIDA INFORMATIVA



Punti della discussione

- Cos'è il Visualizzatore Eventi e a cosa serve.
- Perché è importante configurare il registro di sicurezza.
- Come sfruttarlo per monitorare la sicurezza del sistema.

Cos'è il Visualizzatore Eventi e a cosa serve

Il Visualizzatore Eventi è uno strumento integrato di Windows che registra tutto ciò che accade nel sistema.

Con la categoria "Sicurezza", puoi:

- Monitorare accessi e attività degli utenti.
- Identificare tentativi di accesso non autorizzati.
- Tracciare modifiche a file o configurazioni sensibili.
- È una risorsa essenziale per prevenire rischi, analizzare comportamenti sospetti e migliorare la sicurezza.



Visualizzatore eventi

FileAzioneVisualizza?

Visualizzatore eventi (computer)

Visualizzazioni personalizzate

Registri di Windows

Applicazione

Sicurezza

Installazione

Sistema

Eventi inoltrati

Registri applicazioni e servizi

Sottoscrizioni

Sicurezza

Numero di eventi: 24.018 (!) Nuovi eventi disponibili

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:07:13	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:30	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:06:12	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/11/2024 14:06:12	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:34	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	28/11/2024 14:05:20	Microsoft Windows security auditing.	5058	Other System Events

Evento 4798, Microsoft Windows security auditing.

Generale

Dettagli

È stata enumerata l'appartenenza a un gruppo locale di un utente.

Soggetto:

ID sicurezza:SYSTEM

Nome account:MSIS

Dominio account:WORKGROUP

ID accesso:0x3E7

Nome registro: Sicurezza

Origine: Microsoft Windows security Registrato: 28/11/2024 14:07:13

ID evento: 4798 Categoria attività: User Account Management

Livello: Informazioni Parole chiave: Controllo riuscito

Utente: N/D Computer: MSI

Opcode: Informazioni

Azioni

Sicurezza

Apri registro salvato...

Crea visualizzazione personalizzata...

Importa visualizzazione personalizzata...

Cancella registro...

Filtro registro corrente...

Proprietà

Trova...

Salva tutti gli eventi con nome...

Associa un'attività al registro...

Visualizza

Aggiorna

Guida

Evento 4798, Microsoft Windows security auditing.

Proprietà evento

Associa attività all'evento...

Copia

Salva eventi selezionati...

Aggiorna

Guida

Perché configurare il registro di sicurezza

- Configurare il registro di sicurezza è fondamentale per:
- Monitorare attività sospette: Rileva accessi non autorizzati o modifiche non consentite.
- Prevenire problemi: Permette di intervenire in tempo su potenziali minacce.
- Audit e conformità: Soddisfa normative come GDPR o ISO 27001.
- Conservare prove: In caso di incidenti, i log aiutano a capire cosa è successo.
- Impostare correttamente il registro ti garantisce controllo e sicurezza del sistema.