



oplon®

SECURE ACCESS

NIS2

Oplon Secure Access è un elemento cruciale per supportare la conformità alla direttiva NIS2 in diversi modi. Ecco come Oplon Secure Access può contribuire all'aderenza delle direttive:

1. Gestione degli Accessi Privilegiati

CONTROLLO DEGLI ACCESSI

Oplon Secure Access PAM aiuta a controllare e monitorare gli accessi degli utenti con privilegi elevati, garantendo che solo le persone autorizzate possano accedere a sistemi critici e informazioni sensibili.

PRINCIPIO DEL PRIVILEGIO MINIMO

Consente di implementare il principio del privilegio minimo, assegnando agli utenti solo i permessi necessari per svolgere le loro funzioni specifiche.



2. Monitoraggio e Audit



TRACCIAMENTO DELLE ATTIVITÀ

Registra tutte le attività degli utenti privilegiati, fornendo un audit trail dettagliato che può essere utilizzato per rilevare comportamenti sospetti e rispondere a incidenti di sicurezza.

SEGNALAZIONE DEGLI INCIDENTI

Facilita la segnalazione tempestiva degli incidenti di sicurezza, come richiesto dalla NIS2, grazie alla capacità di monitorare e registrare le azioni degli utenti privilegiati in tempo reale.

3. Sicurezza delle credenziali

GESTIONE DELLE PASSWORD

Automatizza la gestione delle password per gli account privilegiati, garantendo che le credenziali siano sicure e aggiornate periodicamente.

ROTAZIONE DELLE PASSWORD

Implementa la rotazione automatica delle password per ridurre il rischio di compromissione delle credenziali.



4. Controllo degli Accessi Basato su Ruoli (RBAC)

DEFINIZIONE DEI RUOLI

Permette di definire e gestire ruoli e permessi basati sulle esigenze specifiche delle diverse funzioni all'interno dell'organizzazione.

ACCESSI TEMPORANEI

Facilita la concessione di accessi temporanei per attività specifiche, limitando la durata degli accessi privilegiati.

5. Conformità e Reportistica

GENERAZIONE DI REPORT

Fornisce report dettagliati sull'accesso e l'utilizzo delle credenziali privilegiate, utili per le verifiche di conformità e per dimostrare l'aderenza ai requisiti della NIS2.

POLICY DI CONFORMITA'

Aiuta a implementare e mantenere policy di sicurezza che rispondano ai requisiti della NIS2, garantendo che le best practice di gestione degli accessi siano seguite.



6. Risposta agli incidenti



ISOLAMENTO DEGLI INCIDENTI

Consente di isolare rapidamente account compromessi o attività sospette, limitando il potenziale impatto di un incidente di sicurezza.

ANALISI FORENSE

Fornisce dati dettagliati per l'analisi forense post-incidente, facilitando la comprensione delle cause e l'implementazione di misure correttive.

Implementare Oplon Secure Access non solo aiuta a proteggere le informazioni e i sistemi critici, ma è anche un passo significativo verso la **conformità con la NIS2**, contribuendo a rafforzare la sicurezza complessiva dell'organizzazione e a ridurre il rischio di incidenti di sicurezza.

oplon®

Oplon Networks è una società di ingegneria informatica nata nel 2010. La mission è creare prodotti e servizi per garantire Alta Affidabilità e sicurezza a livello infrastrutturale nell'erogazione dei servizi, con standard qualitativi straordinari.

L'eccellenza è il nostro primo obiettivo!

Per questo realizziamo strumenti di cybersecurity e soluzioni integrate per presidiare i moderni Data Center, Network, Cloud e Hybrid Cloud.

Dati e caratteristiche possono variare in qualsiasi momento senza alcun obbligo di preavviso.

Per saperne di più, visita il nostro sito

<https://www.oplon.net>

o scrivi a info@oplon.net

