oplon® SECURE ACCESS NIST

Oplon Secure Access può supportare l'implementazione delle linee guida del NIST in vari modi. Il NIST fornisce una serie di standard e best practice per migliorare la sicurezza informatica e la gestione del rischio, e Oplon Secure Access PAM può aiutare a raggiungere questi obiettivi in modo efficace.
Ecco come Oplon Secure Access può essere di supporto ai principi del NIST:

ACCESS CONTROL - AC

Gestione degli Accessi e Controlli

CONTROLLO DEGLI ACCESSI

Oplon Secure Access aiuta a gestire chi può accedere a sistemi e dati critici, garantendo che solo gli utenti autorizzati possano accedere a risorse sensibili.

PRINCIPIO DEL PRIVILEGIO MINIMO

Implementa il principio del privilegio minimo, assicurando che gli utenti abbiano solo i permessi necessari per svolgere le loro mansioni specifiche, riducendo il rischio di accessi non autorizzati.

IDENTIFICATION AND AUTHENTICATION - IA

Identificazione e Autenticazione

AUTENTICAZIONE FORTE

Supporta l'implementazione di meccanismi di autenticazione robusti, come l'autenticazione a più fattori (MFA), per garantire che solo gli utenti legittimi possano accedere agli account privilegiati.

GESTIONE DELLE IDENTITÀ

Consente una gestione centralizzata delle identità degli utenti privilegiati, migliorando la sicurezza e la tracciabilità delle attività.

(RISK ASSESSMENT - RA)

Gestione del Rischio

VALUTAZIONE DEL RISCHIO

Oplon Secure Access fornisce visibilità sui rischi associati agli accessi privilegiati, aiutando a identificare e mitigare potenziali vulnerabilità.

MONITORAGGIO DELLE ATTIVITÀ

Registra e monitora tutte le attività degli utenti privilegiati, permettendo di identificare comportamenti anomali e potenziali minacce in tempo reale.

AUDIT AND ACCOUNTABILITY - AU

Auditing e Accountability

AUDIT TRAIL

Mantiene un registro dettagliato di tutte le attività eseguite dagli utenti privilegiati, facilitando la conformità con le linee guida del NIST sulla tracciabilità e accountability.

SEGNALAZIONE E REPORTING:

Fornisce report dettagliati sulle attività degli utenti privilegiati, utili per audit di sicurezza e verifiche di conformità.

SYSTEM AND INFORMATION INTEGRITY - SI

Protezione dei Dati e delle Informazioni

PROTEZIONE DELLE CREDENZIALI

Gestisce in modo sicuro le credenziali degli account privilegiati, riducendo il rischio di compromissione delle credenziali.

ROTAZIONE DELLE PASSWORD

Automatizza la rotazione delle password per gli account privilegiati, aumentando la sicurezza delle credenziali.

INCIDENT RESPONSE - IR

Risposta agli incidenti

ISOLAMENTO DEGLI INCIDENTI

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

ANALISI FORENSE

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

SECURITY ASSESSMENT AND AUTHORIZATION - CA

Programma di Sicurezza Continuo

VERIFICHE DI SICUREZZA

Supporta la valutazione continua delle pratiche di sicurezza relative agli accessi privilegiati, contribuendo a garantire che le misure di sicurezza siano efficaci e aggiornate.

POLICY DI SICUREZZA

Aiuta a implementare e mantenere policy di sicurezza coerenti con le linee guida del NIST, assicurando che le best practice di gestione degli accessi siano seguite.

Implementare **Oplon Secure Access** non solo aiuta a proteggere gli asset critici e a gestire gli accessi privilegiati in modo sicuro, ma **supporta anche direttamente l'aderenza agli standard e alle linee guida del NIST**. Questo contribuisce a creare un ambiente informatico più sicuro e conforme alle best practice riconosciute a livello internazionale.

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

oplon®

Per saperne di più, visita il nostro sito
https://www.oplon.net
o scrivici a **info@oplon.net**