oplon® SECURE ACCESS NIS2

Oplon Access is a crucial element in supporting NIS2 directive compliance in several ways.
Here is how Oplon Secure Access can contribute to directive adherence:

1. Privileged Access Management

ACCESS CONTROL

Oplon Secure Access PAM helps control and monitor access of users with elevated privileges, ensuring that only those people authorized can access critical systems and sensitive information.

PRINCIPLE OF THE MINIMAL PRIVILEGE

It allows implementing the principle of minimal privilege, assigning users only the permissions necessary to perform their specific functions.

2. Monitoring and audit

TRACK OF THE ACTIVITIES

Oplon Secure Access records all activities of privileged users, thus providing a detailed audit trail that can be used to detect suspicious behavior and respond to security incidents.

INCIDENT REPORTING

It facilitates timely reporting of security incidents, as required by NIS2, through the ability to monitor and record the actions of privileged users in real time.

3. Security of credentials

PASSWORD MANAGEMENT

Oplon Secure Access automates password management for privileged accounts, ensuring that credentials are secure and updated periodically.

PASSWORD ROTATION

It implements automatic password rotation to reduce the risk of credential compromise.

4. Role based access control (RBAC)

DEFINITION OF ROLES

Oplon Secure Access enables the definition and management of roles and permissions based on the specific needs of different functions within the organization.

TEMPORARY ACCESS

It facilitates the granting of temporary access for specific activities by limiting the duration of privileged access.

5. Compliance and reporting

REPORT GENERATION

Oplon Secure Access provides detailed reports about access and use of privileged credentials, useful for the compliance audits and to demonstrate the adherence to the NIS2 requirements.

COMPLIANCE POLICY

It helps implement and maintain security policies that reply to the NIS2 requirements, ensuring that access management best practices are followed.

6. Incident Reports

INCIDENT ISOLATION

It allows to rapidly isolate compromised accounts or suspicious activities, thus limiting the potential impact of a security incident.

FORENSIC ANALYSIS

It provides detailed data for the post-incident forensic analysys, thus facilitating the understanding of the causes and the implementation of corrective measures.

The implementation of Oplon Secure Access not only helps protect the critical information and systems but is also a significant step toward compliance with NIS2, helping to strengthen the overall security of the organization and reduce the risk of security incidents.

oplon®

Oplon Networks is a computer engineering company founded in 2010. The mission is to create products and services to ensure High Reliability and safety at an infrastructural level in the provision of services, with extraordinary quality standards. **Excellence is our first goal!**
For this we create cybersecurity tools and integrated solutions to preside over modern Data Centers, Networks, Clouds and Hybrid Clouds.

Data and features may change at any time without prior notice.

To find out more, visit our website
https://www.oplon.net
or write to **info@oplon.net**