



# SOC (SECURITY OPERATION CENTER)

## SERVIZIO DI SICUREZZA IT H24

### FASE 1 PRE-ATTIVITÀ



#### PIANIFICAZIONE:

- DEFINIZIONE OBIETTIVI;
- RILEVAZIONE DELLE MINACCE;
- RISPOSTA AGLI INCIDENTI;
- CONFORMITÀ DELLE NORMATIVE.

#### DESIGN DELL'ARCHITETTURA:

- SVILUPPO STRUTTURA SOC;
- SVILUPPO FLUSSI DI LAVORO;
- ASSET INVENTORY.

### FASE 2 IMPLEMENTAZIONE E CONFIGURAZIONE



#### REALIZZAZIONE INFRASTRUTTURA:

- INSTALLAZIONE SONDE E SOFTWARE;
- CONFIGURAZIONE DISPOSITIVI DI RETE E DI SICUREZZA;
- CONFIGURAZIONE DEI TOOL DI MONITORAGGIO;
- VERIFICHE DI ACQUISIZIONE E CORRELAZIONE DEI SISTEMI.

#### MONITORAGGIO E RILEVAZIONE:

- CONFIGURAZIONE AVANZATA DI RULE E SISTEMI DI MONITORAGGIO;
- IMPLEMENTAZIONE USE CASE.

### FASE 3 POST ATTIVITÀ



#### RISPOSTA AGLI INCIDENTI:

- CREAZIONE PROCEDURE E PIANI DI RISPOSTA;
- DEFINIZIONE PROCESSO DI ESCALATION.

#### REPORTING:

- REPORT MENSILI CON INCIDENT RESPONSE.

### VANTAGGI



- SUPPORTO 24/7 DI UN TEAM DI ESPERTI;
- REAL-TIME SECURITY MONITORING (RTSM);
- CONFORMITÀ ALLE NORMATIVE.



**Logos P.A.**  
Fondazione