

Categoria	Descrizione Attività	Frequenza	Responsabile	Conforme a NIS2
Aggiornamento Client VPN	Verificare e aggiornare periodicamente i client VPN su tutti i dispositivi	Mensile	IT Security	Si
Aggiornamento Certificati Proxy	Controllare la validità e aggiornare i certificati SSL/TLS del proxy	Trimestrale	Network Admin	Si
Aggiornamento Jump Server	Applicare aggiornamenti di sicurezza al sistema operativo del jump server	Mensile	Sysadmin	Si
SIEM attivo per VPN	Raccogliere e analizzare log di connessioni VPN tramite SIEM	Continuo	SOC Team	Si
UEBA per accessi remoti	Rilevare comportamenti anomali nelle sessioni remote con UEBA	Continuo	SOC/EDR Analyst	Si
Monitoraggio traffico proxy	Verificare e loggare accessi web e download sospetti tramite proxy	Continuo	Network Admin	Si
Revoca utenti VPN compromessi	Disattivare immediatamente account VPN compromessi o non autorizzati	All'occorrenza	Helpdesk/SOC	Si
Blocco accesso proxy compromesso	Rimuovere accessi LDAP/AD da proxy per utenti compromessi	All'occorrenza	IT Security	Si
Lockdown RDP Jump Server	Chiudere e disabilitare sessioni RDP in caso di comportamento anomalo	All'occorrenza	Sysadmin	Si