MANAGED
CYBER SECURITY

PERIMETRO & ACCESSI

Governare la sicurezza. Ridurre il rischio.

CABER

CABER

MANAGED CYBER SECURITY

CHE COS'È?

Il servizio di Managed Cybersecurity è pensato per supportare le aziende nella gestione continuativa della sicurezza del proprio perimetro digitale e degli accessi dall'esterno.

L'obiettivo è ridurre il rischio operativo e garantire continuità, attraverso un approccio strutturato che combina configurazione, monitoraggio, aggiornamenti e controllo periodico.

Il servizio si concentra in particolare su:
gestione degli apparati di sicurezza e di rete
gestione degli accessi remoti e delle relative policy

CABER

MANAGED CYBER SECURITY

OBIETTIVI & RISULTATI

Il servizio è progettato per ottenere risultati concreti e misurabili:

Riduzione del rischio
Limitazione delle superfici di esposizione dall'esterno, controllo degli accessi e mitigazione dei rischi legati a credenziali compromesse o configurazioni non aggiornate.

Continuità operativa
Monitoraggio costante, patch pianificate, configurazioni coerenti e interventi tempestivi in caso di necessità.

COSA COMPRENDE IL SERVIZIO?

Il servizio si articola in due aree principali, strettamente integrate tra loro:

1

Gestione del perimetro di rete

Firewall e apparati di sicurezza gestiti nel tempo, secondo best practice condivise.

2

Gestione degli accessi dall’esterno

Accessi remoti governati tramite policy chiare, tracciate e periodicamente verificate.

CABER

GESTIONE FIREWALL & APPARATI DI RETE

Il servizio prevede la gestione continuativa degli apparati che costituiscono il perimetro di rete aziendale.

Attività incluse

- **inventario degli apparati gestiti** (firewall, router, switch L3, access point ove necessario)
- **hardening di base e messa in sicurezza dell'accesso amministrativo**
- **gestione delle configurazioni:**
  - regole firewall e NAT
  - segmentazione VLAN, se presente
  - policy DNS e logging secondo quanto concordato
- **aggiornamenti:**
  - firmware e patch pianificate con finestra di manutenzione
  - interventi su vulnerabilità critiche secondo SLA
- **backup delle configurazioni e supporto al ripristino**
- **report mensile con stato della sicurezza e modifiche effettuate**

SERVIZI OPZIONALI

- configurazioni in alta affidabilità
- IDS/IPS e tuning
- web e DNS filtering
- gestione Wi-Fi enterprise

GESTIONE ACCESSI ESTERNI & POLICY

Il servizio include il censimento e la gestione strutturata di tutti i punti di accesso dall'esterno.

Attività incluse

- **mappatura dei punti di ingresso** (VPN, port forwarding, RDP, SSH, portali, accessi cloud)

- **riduzione della superficie esposta:**
  - revisione dei port forwarding esistenti
  - chiusura di accessi non più necessari

- **accesso remoto standardizzato:**
  - VPN con autenticazione a più fattori
  - policy per gruppi e ruoli aziendali

- **gestione delle policy di accesso:**
  - principio del minimo privilegio
  - accessi fornitori temporanei, tracciati e revocabili

- **logging degli accessi e segnalazione di eventi anomali**

SERVIZI OPZIONALI

- ZTNA e accesso per applicazione
- bastion/jump server
- gestione semplificata delle credenziali privilegiate

CABER

ONBOARDING INIZIALE (una tantum)

Il servizio parte sempre da una fase di onboarding strutturata

1. **Assessment iniziale dell’infrastruttura**
2. **Raccolta dei requisiti di accesso dall’esterno**
3. **Normalizzazione delle configurazioni e definizione della baseline**
4. **Attivazione di monitoraggio, backup e procedure operative**
5. **Redazione del documento “Accessi dall’esterno”**

OUTPUT DELL’ONBOARDING

- BASELINE SECURITY REPORT
- PIANO DI AZIONE DEI PRIMI 30 GIORNI

CABER

ATTIVITÀ CONTINUATIVE INCLUSE

- GESTIONE TICKET E CHANGE LOG
- PROGRAMMAZIONE CONDIVISA DEGLI AGGIORNAMENTI DI SICUREZZA
- REPORT PERIODICO
- REVISIONE TRIMESTRALE DEGLI ACCESSI ATTIVI

CABER

LIVELLI DI SERVIZIO (SLA)

Il servizio è disponibile in diversi livelli, calibrati in base alle dimensioni e alle esigenze dell'organizzazione.

ESSENZIALE

- monitoraggio base e backup configurazioni
- patch pianificate
- gestione regole e VPN su richiesta
- report mensile
- disponibilità in orario d'ufficio

BUSINESS

- servizi del pacchetto Essenziale
- alerting su eventi critici
- revisione accessi trimestrale
- presa in carico rapida

PREMIUM

- servizi del pacchetto Business
- disponibilità H24
- gestione immediata delle urgenze critiche
- tuning avanzato di policy e sistemi di sicurezza
- revisione accessi mensile

CABER

FORMAZIONE SPECIFICA

Non un corso teorico, ma un percorso pratico e mirato, pensato per rafforzare i comportamenti quotidiani che incidono realmente sulla sicurezza aziendale.

La formazione è progettata per affiancare il servizio di cybersecurity gestita e renderlo efficace anche sul piano organizzativo e umano.

La formazione è organizzata per cicli, adattabili al contesto aziendale:

- Ciclo iniziale (Onboarding)
- Attivato entro 30–60 giorni dall'avvio del servizio.
- Richiamo periodico
- Annuale o semestrale nei contesti più esposti.
- Materiali di supporto
- Micro-pillole tematiche (documenti brevi, video o podcast) fruibili in autonomia e in modo controllato.
- Verifica e tracciabilità
- Attestazione interna e registro di partecipazione.

MODULI FORMATIVI

I contenuti sono differenziati in base alle responsabilità e alle mansioni.

TUTTI I DIPENDENTI
modulo base
(30 – 90 MINS)

- Phishing e social engineering (email, WhatsApp, “finto tecnico”)
- Password e passphrase
- MFA: cosa fa e cosa non fa
- Link, allegati, QR code e condivisioni sospette
- Indicazioni pratiche su cosa fare nei primi minuti in caso di sospetto incidente

AMMINISTRAZIONE/HR
dati sensibili
(60 MINS)

- PEC, fatture e principali frodi (CEO fraud, cambio IBAN)
- Gestione documenti e condivisioni
- Riservatezza e minimizzazione dei dati
- Approccio pratico, orientato all’operatività quotidiana.

TECNICI/IT/KEY USER
(90 – 120 MINS)

- Accesso remoto sicuro (VPN, eventuali jump host)
- Gestione delle credenziali amministrative e superamento degli account condivisi
- Aggiornamenti e vulnerabilità: criteri di priorità e finestre di intervento
- Analisi dei log: cosa osservare quando emergono anomalie

DIREZIONE/RESPONSABILI
(45 – 60 MINS)

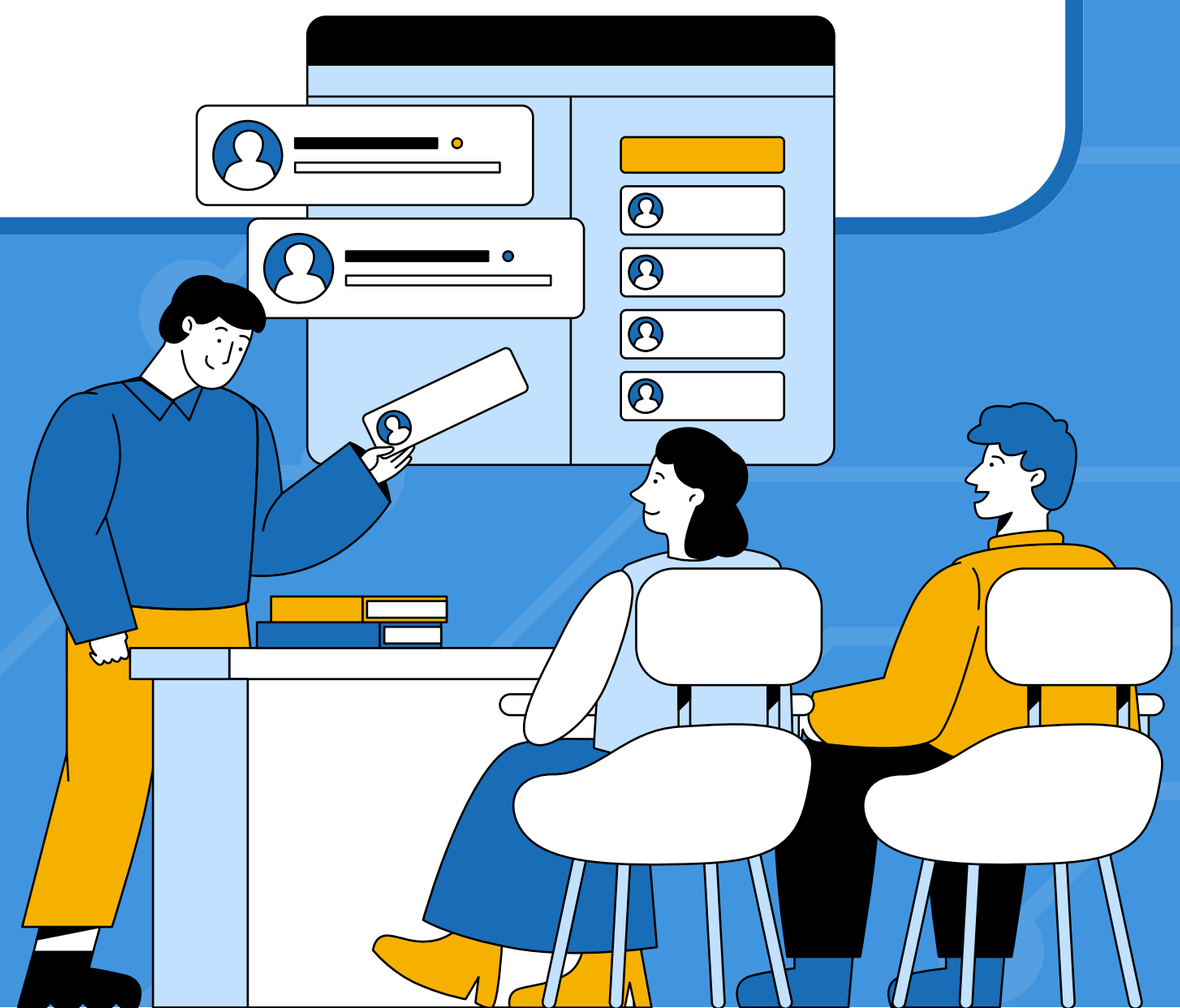
- Rischi e impatti sul business
- (fermo operativo, perdita dati, reputazione)
- Processi decisionali in caso di incidente
- Ruoli, escalation e comunicazioni
- KPI di sintesi per il monitoraggio della sicurezza
- (MFA attivo, accessi esterni ridotti, utenti formati, incidenti evitati)

CABER

DELIVERABLE POST FORMAZIONE

Al termine del percorso vengono forniti:

1. **Piano formativo annuale per mansione**
2. **Materiale sintetico** (1–2 pagine per modulo)
3. **Registro dei partecipanti e risultati delle verifiche**
4. **Report conclusivo con aree critiche emerse e azioni correttive suggerite** (policy, procedure, miglioramenti organizzativi)



CABER Managed Cyber Security v. 2026-01

+39 0522 550 802 info@caber.srl www.caberinformatica.com