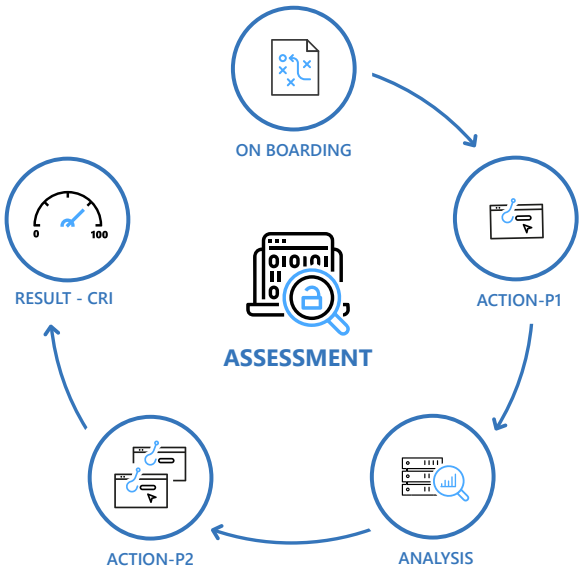
CYBER Pro
Powered by PCS Group

Security Assessment

Fornisce un indicatore del tuo livello di rischio informatico



Il Security Assessment consente di analizzare a 360° il rischio di esposizione ad attacchi informatici ed è la fase iniziale di un percorso che consente di misurare in modo preciso i potenziali punti di attacco e carenze di sicurezza.

Per ogni area analizzata viene indicato il Fattore di Rischio (CRI) e vengono indicate le potenziali Remediation da adottare fornendo documentazione di analisi tecnica e di valutazione Management

CYBER RISK INDEX (CRI)

Come misuriamo il rischio

Il **CRI** è un indicatore che misura il rischio di esposizione ad attacchi informatici.
Il Valore varia da **0 (rischio basso)** a **100 (rischio molto elevato)**.

Ogni area analizzata in fase di Assessment **riceve un valore di CRI** che creerà un **CRI globale** per identificare il livello di rischio a cui l'azienda è esposta.

Le successive fasi di **Remediation** puntano alla riduzione dell'indicatore.

LE FASI

ON BOARDING

- Raccolta informazioni Tecniche dell'infrastruttura
- Raccolta informazioni su procedure esistenti ed aspetti normativi
- Definizione Strategia di Attacco Phishing fase 1 e fase 2
- Definizione Strategia di Attacco BAITING

> È importante che solo le persone strettamente necessarie dell'azienda siano a conoscenza dell'attività in corso.

ACTION – Phase 1

- Attivazione prima campagna di Phishing
- Vulnerability Assessment Interno ed Esterno
- Consegna/Posizionamento delle esche relative ad attacco BAITING
- Analisi tecnica delle potenziali superfici di attacco

- Perimeter
- Wired Network
- Wireless Network
- Active Directory
- End Point
- Backup & DR
- Log Management & SIEM
- EMAIL
- IOT
- Physical Security
- Additional Services
- Legal & Procedures

ANALYSIS

- Vulnerability Assessment Interno ed Esterno
- Analisi tecnica dell'infrastuttura aziendale
- Definizione delle Remediations applicabili

ACTION – Phase 2

- Si presume che in questa fase molto del personale dell'azienda sia venuto a conoscenza delle attività in corso.
- Si procede pertanto ad un secondo attacco di Phishing per misurare la consapevolezza e del personale alla luce delle attività in corso.
- Il dato in rapporto alla prima campagna di phishing fornirà una chiara visione dell'Awareness del personale in ambito Cyber Security

RESULT = CRI

- Incontro finale nel quale vengono presentate le risultanze dell'assessment.
- Presentazione del documento Executive
- Presentazione del Documento tecnico
- Illustrazione delle remediation