

CyberRisk Monitoring



Il servizio CyberRisk Monitoring, attraverso strumenti di analisi degli asset informatici, ha l'obiettivo di fornire un riscontro credibile sull'effettivo grado di rischio di attacco cyber delle Organizzazioni e fornire alert su rischi cyber interni ed esterni all'azienda nel periodo di tempo monitorato.

I principali destinatari del servizio CyberRisk Monitoring sono tutte le aziende che considerano la corretta gestione degli asset informatici una questione di estrema importanza e che sono interessati a proteggere i propri asset da eventuali attacchi esterni attraverso l'utilizzo di strumenti di monitoraggio e analisi preventive basate su competenze specifiche. In particolare:

Aziende del settore Banking e Insurance con l'obiettivo di proteggere le transazioni finanziarie e l'integrità dei dati dei propri clienti e migliorare la credibilità e fiducia dei consumatori perché consapevoli che se il rischio cyber è monitorato si possono evitare perdite economiche per le banche, per i correntisti e le aziende corporate.

Aziende del settore Transportation con l'obiettivo di monitorare le vulnerabilità dei sistemi automatizzati di automezzi, velivoli e treni, in quanto il rischio di un eventuale cyber-attack può minare la sicurezza dei trasportati.

Aziende del settore Sanitario con l'obiettivo di monitorare le vulnerabilità dei sistemi automatizzati, principalmente per quanto riguarda i software medicali, al fine di garantire alti livelli di sicurezza dei pazienti.

Multinazionali o grossi gruppi di aziende con l'obiettivo di monitorare in modo accentrato le vulnerabilità dei propri sistemi informatici distribuiti sul territorio o ramificati in diversi paesi, al fine di tutelare e salvaguardare il patrimonio aziendale nella sua globalità.

L'obiettivo del servizio di **CyberRisk Monitoring** è quello di identificare e analizzare i rischi di un'organizzazione nella sua complessità, in ambito cybersecurity, in un dato periodo temporale, attraverso strumenti di analisi e attività di valutazione on-site dei punti di forza e debolezza del sistema dei controlli messi in atto per prevenire i rischi, con successivo follow-up degli stessi in accesso remoto.

Tramite l'utilizzo di un software specifico, è possibile fornire al cliente avvisi proattivi e una visione completa dei rischi cyber interni ed esterni all'azienda. Lo strumento di monitoraggio, infatti, evidenzia le potenziali lacune di sicurezza.

**Ufficio Commerciale Certificazione Sistemi
Kiwa Italia**
certificazione.sistemi@kiwacermet.it
+39 0514593111

Il servizio consiste nelle seguenti attività:

- Analisi dei reali rischi cyber dell'azienda, svolta in accesso remoto sui sistemi scelti dal cliente, tramite un applicativo software ad hoc per un dato periodo di tempo.
- Elaborazione dei risultati e produzione di un report per evidenziare il livello di rischio cyber del cliente.
- Attività di follow-up dei rischi, effettuata in accesso remoto tramite applicativo ad hoc, successivamente alla prima rilevazione, per verificare la tenuta dei controlli nel tempo.