CYBER SECURITY DIVISION

SMART WORKING CYBER KIT

6 Aprile 2020

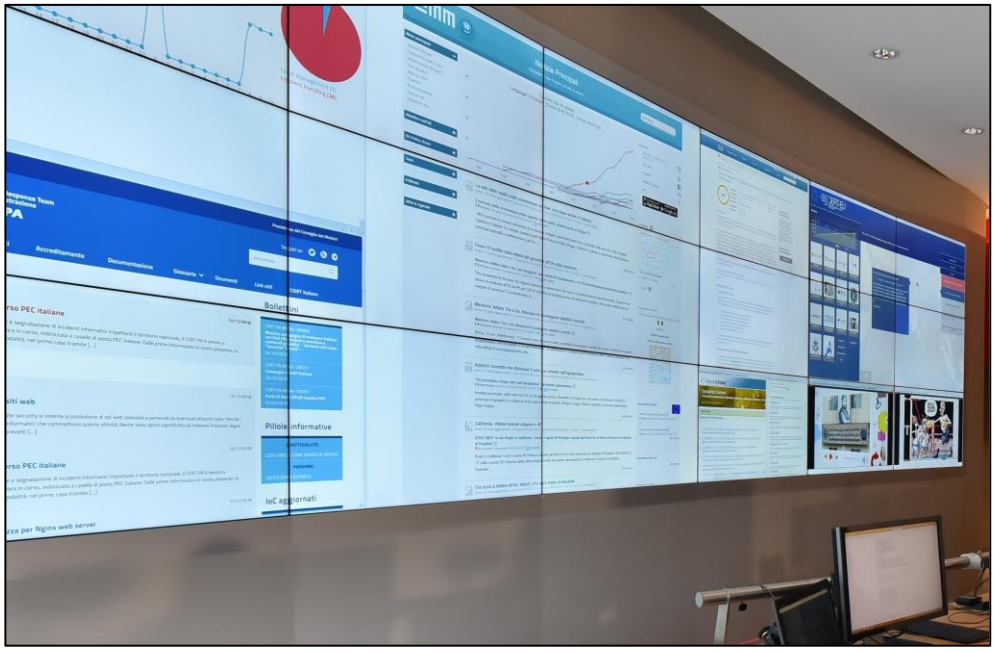
LEONARDO

PREMESSA

Nella difficile fase di emergenza sanitaria che stanno attraversando i nostri Paesi, Leonardo ha intrapreso una serie di iniziative per sostenere lo sforzo di tutti coloro che sono impegnati quotidianamente nella gestione e nel contenimento dell'epidemia da COVID-19 e delle persone che lavorano per mantenere il più possibile una resilienza operativa di aziende ed istituzioni.

In questo contesto si inserisce lo *Smart Working Cyber Kit*: a partire dal 6 aprile, Leonardo offre gratuitamente per 2 mesi un servizio di ***Threat Intelligence,*** specificatamente progettato per supportare le aziende a migliorare la propria difesa rispetto alle minacce cibernetiche legate alle tematiche COVID-19, in questa fase di maggiore esposizione dovuta al ricorso massivo allo smart working.

Il servizio, garantito dalla Divisione Cyber Security, sarà erogato alle prime **100 aziende** che ne richiederanno l'utilizzo e permetterà di monitorare le principali minacce cibernetiche contro i sistemi, le applicazioni e le reti che garantiscono ai dipendenti l'accesso da remoto alle infrastrutture aziendali e coprire quindi eventuali vulnerabilità connesse.



Leonardo Security Operation Center

IL KIT

Lo *Smart Working Cyber Kit* è una sintesi della metodologia e dell'approccio operativo di Leonardo per la protezione delle infrastrutture IT ed è lo strumento con cui vogliamo condividere la nostra esperienza ed aiutare a proteggere le risorse di chi si rivolge a noi in questo momento critico.

Lo facciamo grazie a tre strumenti principali:

1. **Documento Informativo**: il documento ha lo scopo di rendere consapevoli tutti gli impiegati delle minacce di vulnerabilità che possono scaturire dall'uso intensivo dello smart working e, al contempo, si rivolge ai team operativi per guidarli in un rapido ed efficace assessment. Ovvero:
   - implementare attività di assessment,
   - eseguire l'analisi del rischio,
   - definire politiche e procedure di sicurezza appropriate,
   - implementare attività finalizzate alla creazione di una maggiore awareness della popolazione aziendale rispetto ai rischi cyber,
   - implementare un real time security monitoring process.

2. **Video Corso di Awareness**: Il video corso è indirizzato all'intera popolazione aziendale che lavora da remoto, dagli impiegati ai manager, ed è un utile supporto per la formazione dei remot workers per lavorare in modalità più sicura. Lo scopo del video è di aumentare la consapevolezza dei lavoratori nei confronti dei rischi derivanti dalle principali minacce cyber, favorendo al contempo una loro migliore security posture e aumentando conseguentemente la resilienza dell'intera organizzazione. La consapevolezza dei rischi diventa fondamentale nello scenario operativo che si è creato a causa dell'emergenza COVID-19.

3. **Threat Intelligence (Early Warning) Service**: il servizio è pensato per supportare aziende pubbliche e private che forniscono servizi essenziali al Paese. Ha lo scopo di fornire alle aziende report periodici alimentati da un sistema di Threat Intelligence in grado di monitorare in tempo reale le fonti aperte (web, deep web, darkweb) per identificare possibili nuove minacce cibernetiche legate alle tematiche COVID-19 o vulnerabilità associate ai sistemi utilizzati per lo smart working.

COME ACCEDERE AL SERVIZIO

Il servizio viene erogato gratuitamente per 2 mesi alle prime 100 aziende che ne richiedono l'utilizzo, mediante la compilazione di un modulo di consenso in cui il richiedente, insieme alle informazioni identificative (nome, cognome, indirizzo email), fornisce anche alcune informazioni sulle caratteristiche salienti dell'azienda interessata al servizio per una migliore profilazione.

Leonardo Intelligence Operation Center

Il servizio è fruibile al link: **https://cybersecurity.leonardocompany.com/access**.

Piazza Monte Grappa, 4
00195 Rome
T +39 06324731
F +39 063208621

leonardocompany.com