BONUS:

Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto. Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC. Il file "sospetto" è iexplore.exe contenuto nella cartella C:\Programmi\Internet Explorer .

Come membro senior del SOC ti è richiesto di convincere il dipendente che il file non è maligno.

Esercizio:

Possono essere usati gli strumenti di analisi statica basica e/o analisi dinamica basica visti a lezione. No disassembly no debug o similari VirusTotal non basta, ovviamente Non basta dire iexplorer è Microsoft quindi è buono, punto.

Oltre VirusTotal come già suggerito dalla traccia possiamo eseguire le seguenti azioni per determinare se l'eseguibile "sospetto" iexplorer.exe è un file maligno:

Analisi Statica Basica

-Calcoliamo l'hash del file "iexplore.exe" usando "md5deep" e confrontiamolo con quello disponibile nei repository ufficiali di hash delle applicazioni Microsoft per verificarne l'integrità.

-Facciamo click con il tasto destro del mouse sul file che vogliamo analizzare e apriamo le "Proprietà" per verificare che il produttore sia Microsoft Corporation.

Analisi Dinamica Basica

-Utilizziamo Wireshark monitorando le connessioni di rete stabilite da "iexplore.exe". Che saranno verso server legittimi di Microsoft o altri siti web validi.

-Usiamo Process Explorer per analizzare il processo iexplore.exe. Possiamo osservare le DLL caricate, i thread attivi e altre informazioni utili per assicurarci che il comportamento del processo sia quello atteso per un browser legittimo.