

ESERCIZIO W19D1 PARTE 2

Quanti e quali sono i livelli su cui è basato il sistema di valutazione di ThreatConnect? Compila una lista spiegando, per ogni livello, le caratteristiche:

- Minaccia confermata (90-100%)

Significa che la minaccia viene approvata come tale, le fonti trovate in questo caso non lasciano dubbi sulla sua autenticità.

- Minaccia probabile (70-89%)

Significa che la minaccia non è ancora stata confermata, anche se le informazioni raccolte la certificano come tale

- Minaccia possibile (50-69%)

La tempestività risulta in linea con la minaccia attuale, ma mancano ancora delle voci solide al riguardo.

- Minaccia incerta (30-49%)

Valutazione possibile, ma servono più informazioni che confermino la possibilità di una minaccia.

- Minaccia improbabile (2-29%)

Valutazione possibile, ma non si trovano informazioni utili sulla rete.

- Minaccia screditata (1%)

La minaccia non esiste

Tekdefense – prova il software

Sfortunatamente, gli endpoint di questo Cyber threat intelligence tool risultato non utilizzabili. Ai giorni d'oggi, se vogliamo utilizzare strumenti equivalenti possiamo ricorrere a siti come ipvoid per saggiare certi indirizzi ip, file, oppure url sospetti oppure VirusTotal.

The screenshot displays the VirusTotal web interface for the IP address 37.221.161.215. The interface is dark-themed. At the top, a search bar contains the IP address. Below the search bar, a circular progress indicator shows a score of 2/91. A warning message states: "2/91 security vendors flagged this IP address as malicious". The IP address is listed as 37.221.161.215 (37.221.160.0/20) and AS 3223 (Voxility LLP). A button labeled "Analyze VirusTotal" is visible. The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A banner encourages joining the VT Community. Below, a table titled "Security vendors' analysis" shows results from various vendors. The table has two columns for vendor names and their analysis results. The results are as follows:


Vendor	Analysis Result
Dr.Web	Malicious
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Antiy-AVL	Clean
benkow.cc	Clean
MalwareURL	Malware
Acronis	Clean
AILabs (MONITORAPP)	Clean
alphaMountain.ai	Clean
Avira	Clean
Bfore AI PreCrime	Clean

37.221.161.215

Check IP Address

IP Address Information

analisi ipvoid

Analysis Date	2024-03-14 13:22:45
Elapsed Time	6 seconds
Detections Count	1/101
IP Address	37.221.161.215 Find Sites IP Whois
Reverse DNS	Unknown
ASN	AS3223
ISP	Voxility S.R.L.
Continent	Europe
Country Code	 (RO) Romania
Latitude / Longitude	Google Map
City	Bucharest
Region	Bucuresti