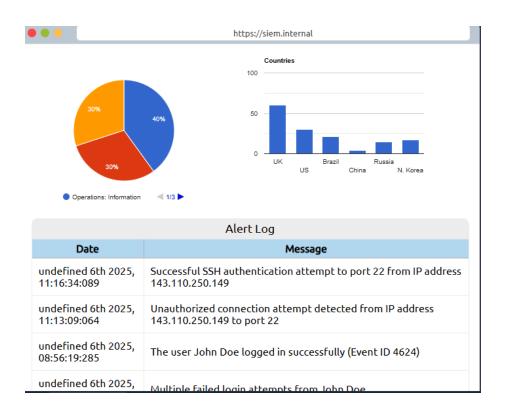
Lab Activity on defensive security and related topics, such as Threat Intelligence, SOC, DFIR, Malware Analysis, and SIEM.

Determine malicious alert from the alert log?



The unauthorized connection attempt detected from IP address 143.110.250.149 to port 22,is suspicious to be malicious. I need to investigate further by using an open source database like AbuseIP DB or Cisco Talo intelligence to confirm if the alert is malicious.



IP-SCANNER.THM

Check by IP Address

143.110.250.149

Submit

➤ The result from the scan shown below confirms the IP address is malicious, so I have to escalate to team lead and wait for authorization to block this IP address on the firewall.





IP-SCANNER.THM

143.110.250.149 was found in our database!

Confidence of the IP being malicious is 100%

Malicious

ISP China Mobile Communications Corporation

Domain Name chinamobileltd.thm

Country China

City Zhenjiang, Jiangsu

➤ I filled out the malicious IP address of the firewall block list and clicked on block IP address.



Firewall Block List

Block List	
Date	IP Address
July 2nd 2021, 13:27:00:948	101.34.37.231
June 30th 2021, 09:12:11:857	212.38.99.12
June 23rd 2021, 23:56:28:370	213.106.84.35

143.110.250.149 Block IP Address

You blocked the malicious IP address!

THM{THREAT-BLOCKED}

> A report was written stating the IP address, the time of the event,all steps taken to verify if the IP address is malicious and action taken.