SOC Simulator

rlcmtech200

Victory! Security breach prevented!

You passed the scenario by identifying all true positive alerts. Your MTTR and dwell time were longer than average, with a "Phishing" alert taking notably longer to close. Your true positive rate improved to 60%, better than your previous runs.

🏆 1st ⌃ 0   ⊕ 165 pts + 165 pts

True positives

Assess your accuracy on the alerts you marked as true positives.

✦ **Overall analysis** POWERED BY AI

Your reports provide a good level of detail, but there are areas where clarity and completeness can be improved. While you have covered the 'What' and 'Why' aspects well, the 'Who' and 'Where' could be more explicitly detailed to enhance understanding. Additionally, ensure that the 'When' is consistently clear across all reports to maintain a coherent timeline of events. Focusing on these areas will help in creating more comprehensive and actionable reports.

https://tryhackme.com/soc-sim/public-
summary/190da5ecea0d029cb0e2dcff3e92b652492a0a345ab6ba9c7c493e49052cbafb6577a331cc44d8
a7ac963aa814f17591?fbclid=IwY2xjawOYtJVleHRuA2FlbQIxMQBzcnRjBmFwcF9pZBAyMjIwMzkxNzg4Mj
AwODkyAAEe1ByHAANsF4_1-bjGdoRUXId41bEne9WT5-Ruk-
Y0DxxYBv9iID93jAtGRY4_aem_5nQHgdvOikuK66eSZu3MLw