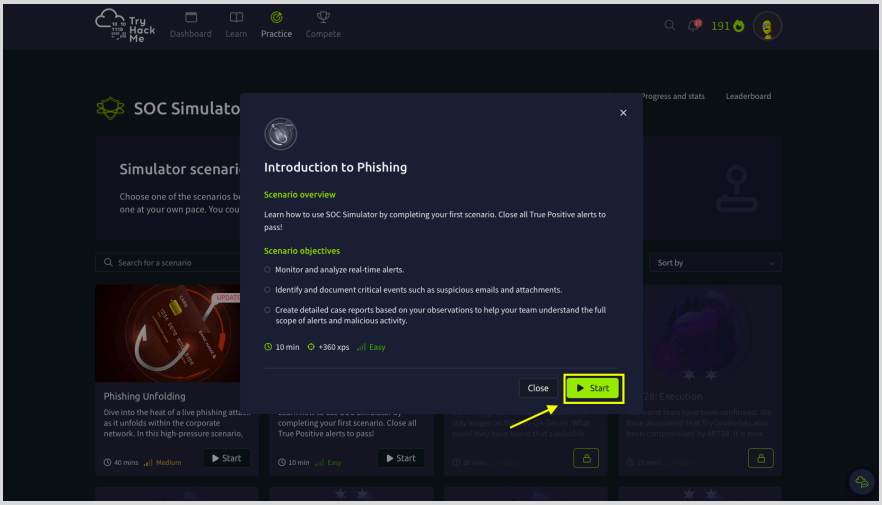
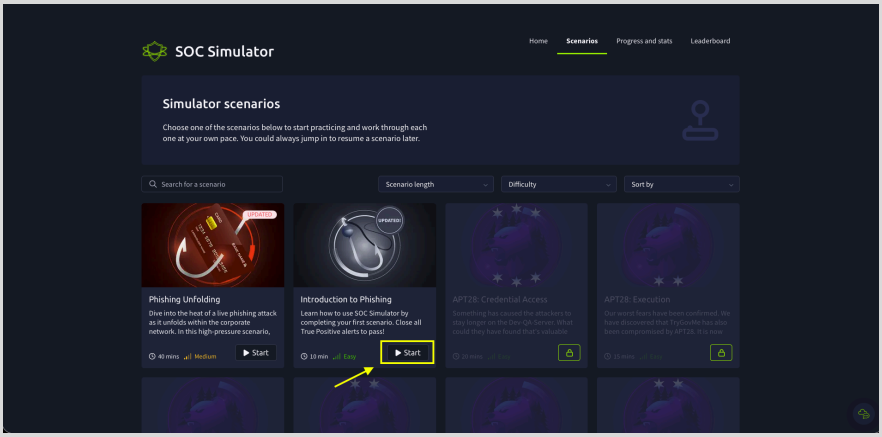
SOC Simulator

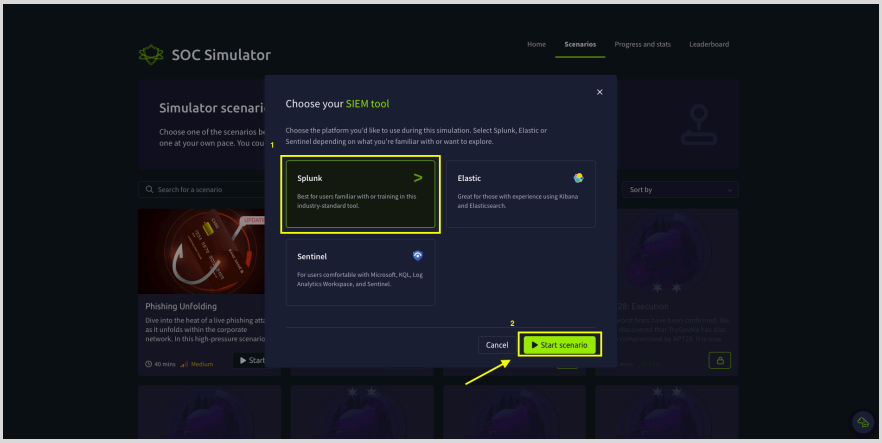
1. Launch simulator



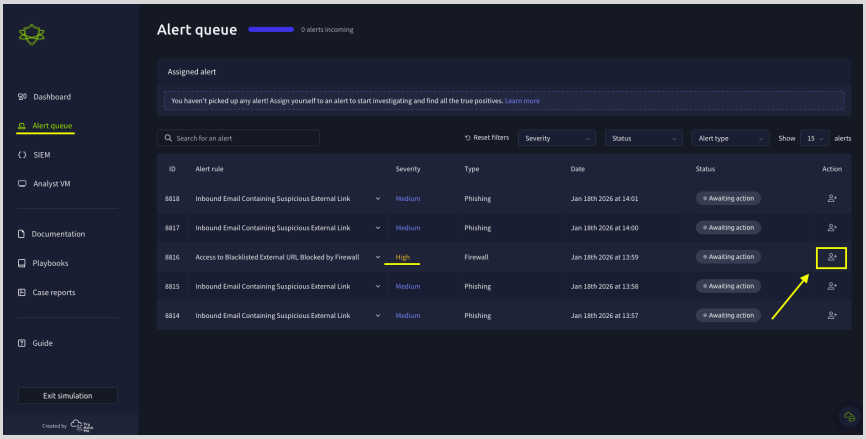
2. Choose exercise (Introduction to Phishing SOC Simulation)



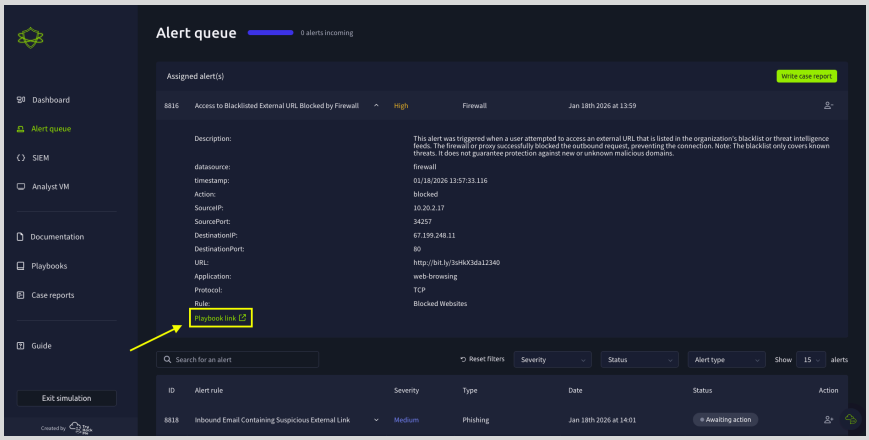
3. Choose SIEM tool (Splunk)

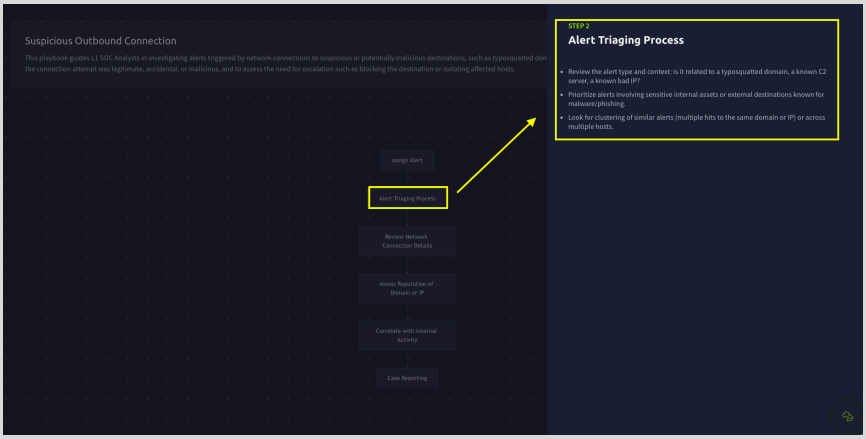


4. Go to **Alert Queue** board
5. Assign yourself an **alert** (prioritize by Severity & Date/Time)

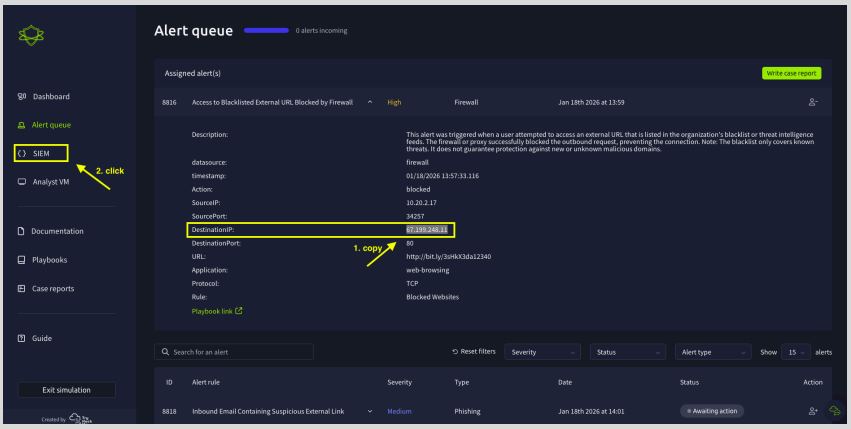


6. Click **Playbook** link for triaging guide

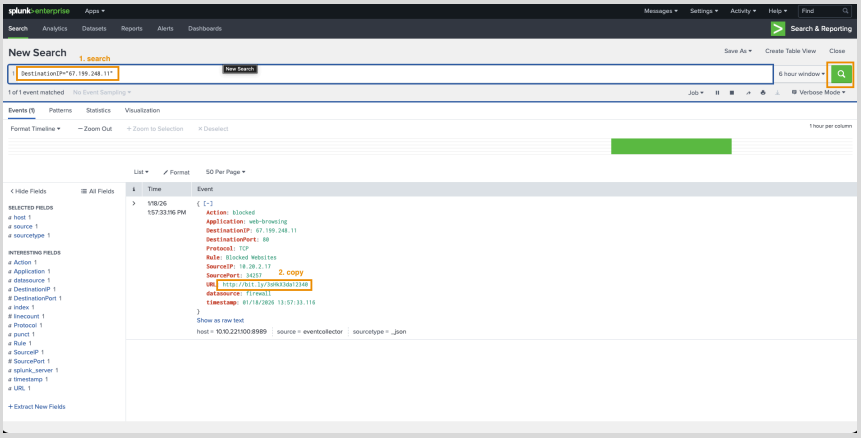




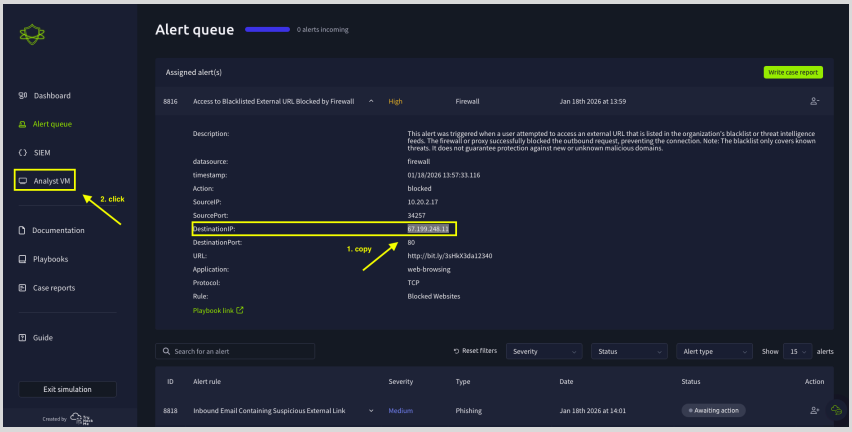
7. Take note of the IOCs (Indicators of Compromise) for investigation
8. Click **SIEM** tab for investigation.



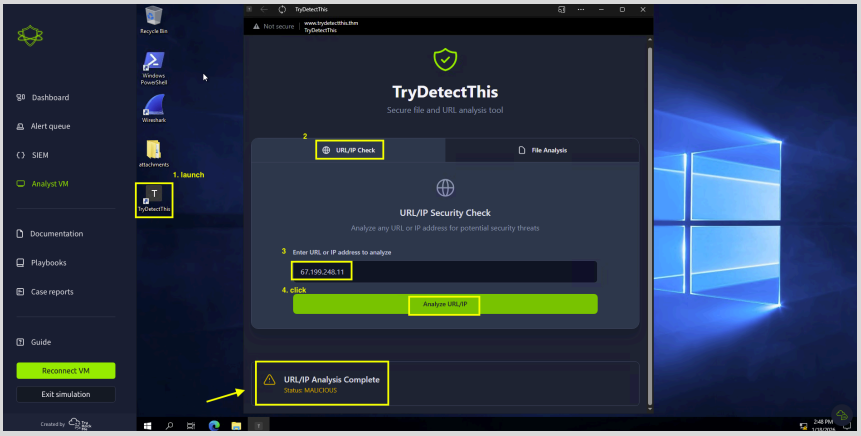
9. Search/Investigate using SIEM (Splunk) for additional information



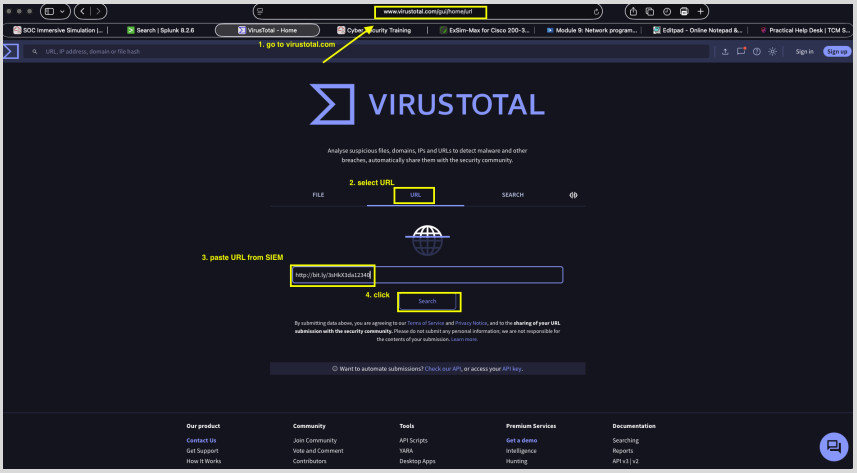
10. Click Analyst VM to investigate if files, IPs, and/or URLs are malicious.

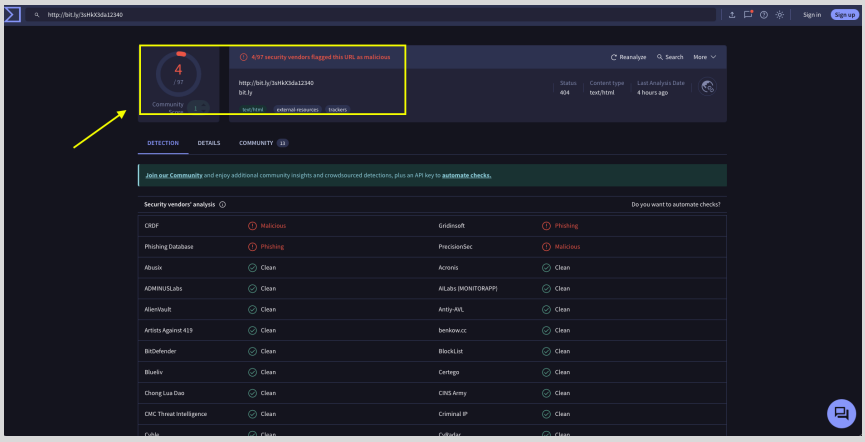


11. Launch TryDetectThis tool (THM Investigation Tool) > enter suspicious IP or URL to investigate.

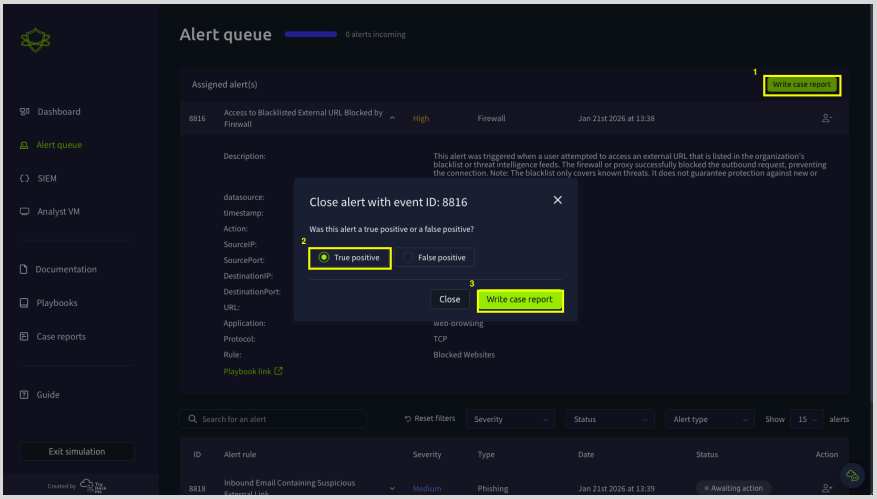


12. Use other available tools (ex. VirusTotal) if needed to investigate

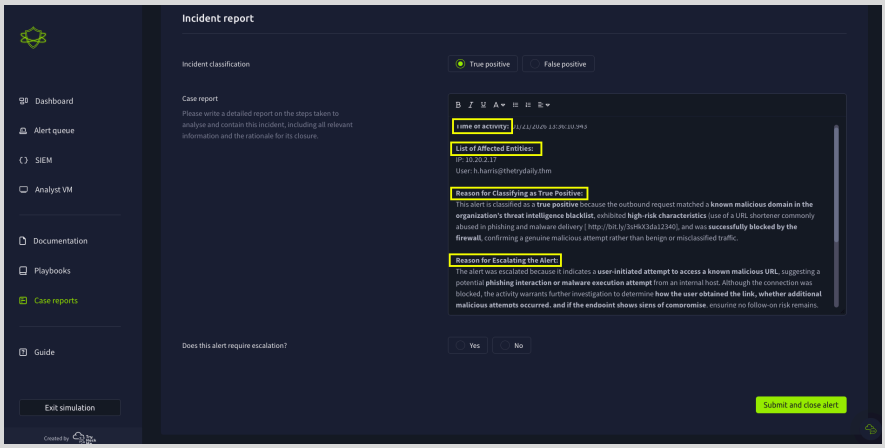




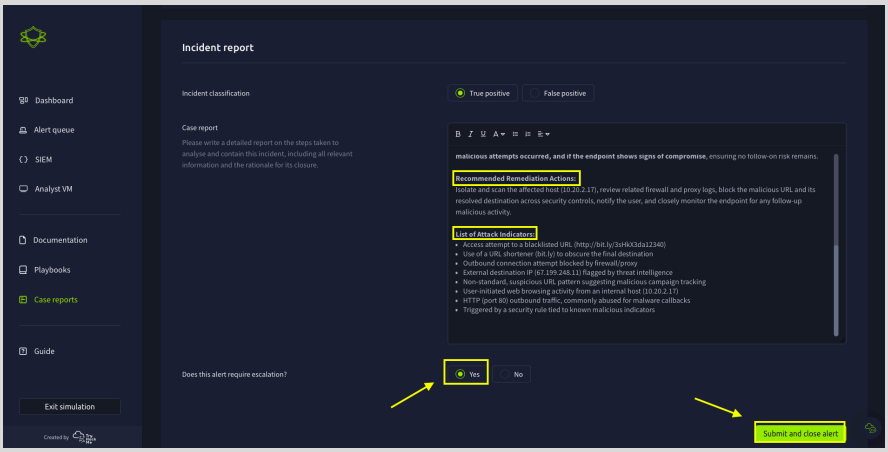
13. Click **Write case report**: Specify if alert is True Positive or False Positive.



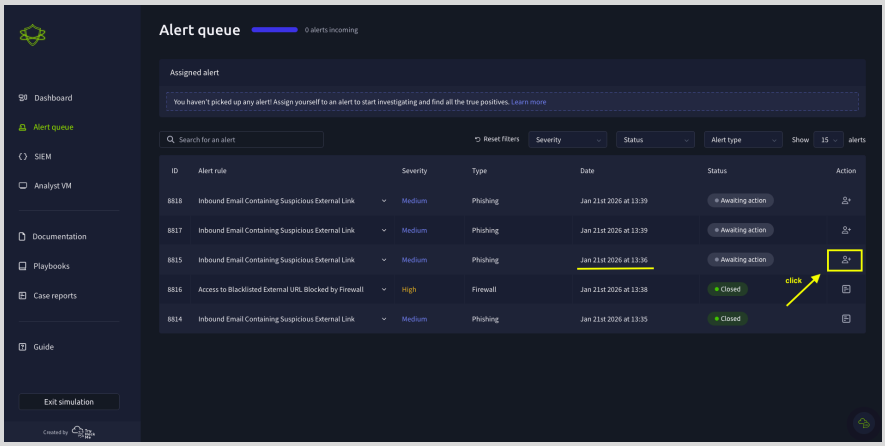
14. Write a thorough **incident report** : clearly document **who was affected, what happened, when and where it occurred, why it's significant, and how it was detected and remediated**, using concise, factual language that can be understood by both technical and non-technical stakeholders.

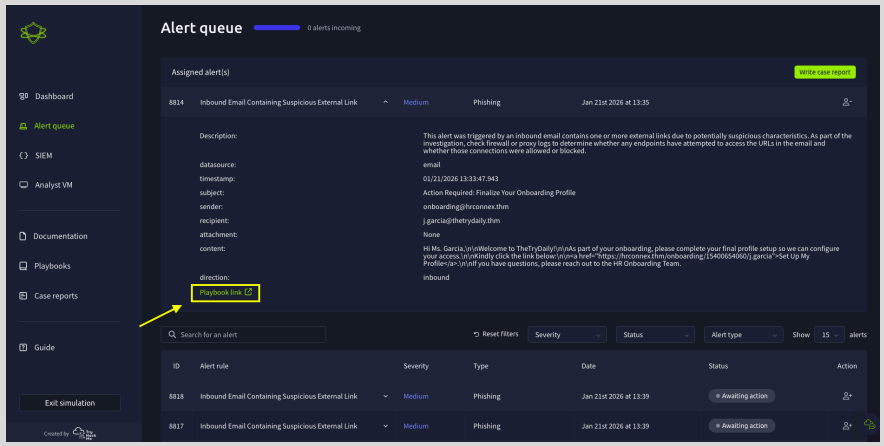


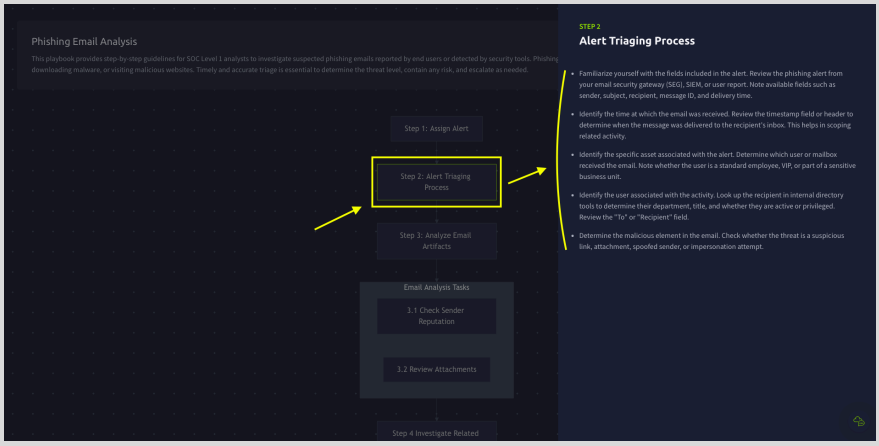
15. **If an event needs to be escalated**, specify the reason, select **Yes** radio button, then click **Submit and close alert.**

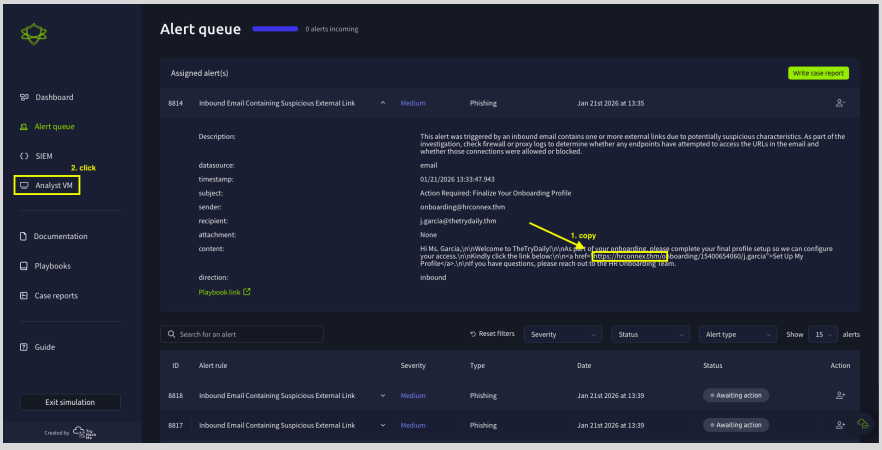


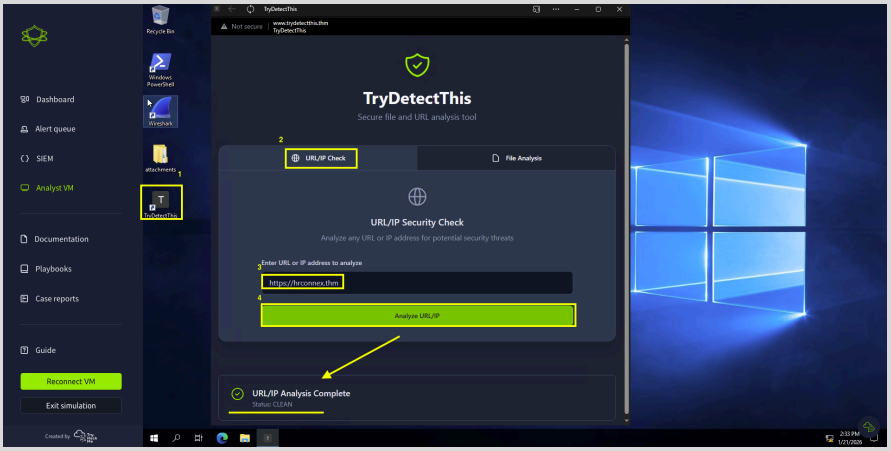
16. Assign yourself another **alert** (prioritize by Severity & Date/Time) and **repeat the whole investigation and triaging process**.



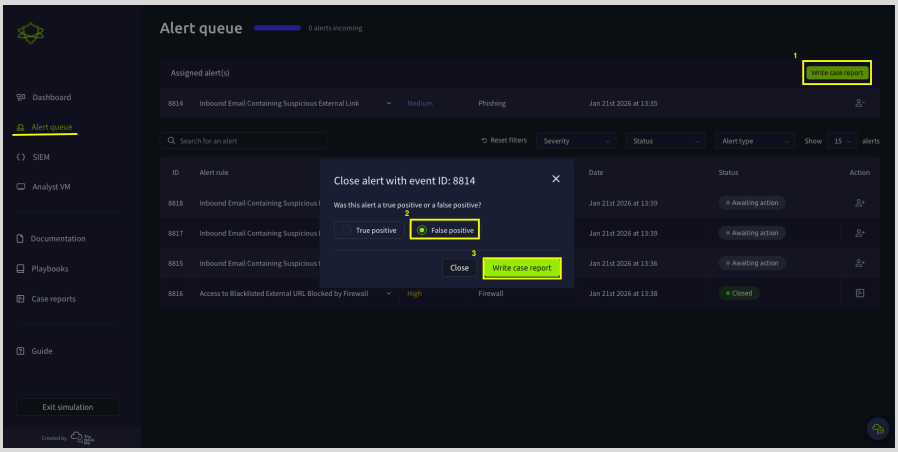




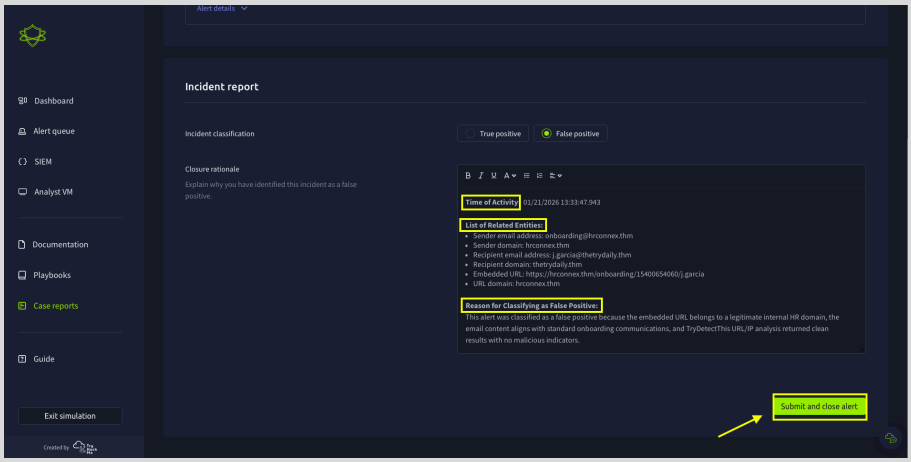




17. Click **Write case report**, then Check **False Positive** in this case.



18. Write a thorough **incident report**, then click **Submit and close alert**



19. On to the **next alert** (prioritize by Severity & Date/Time) and **repeat the previous process.**