Cybersecurity Tabletop Exercise Report

Tabletop Facilitator: ChatGPT | Participant: Brandon Jones

Date: July 26, 2025

Scenario Overview

You were placed in the role of a junior cybersecurity analyst interning at a mid-sized healthcare organization. An alert from the SIEM system indicated large outbound traffic to a foreign IP. You were tasked with identifying, responding to, containing, and reporting the incident in stages.

Key Decisions & Responses

Q1: What is the first thing you do upon receiving an alert?

Response: Refer to the incident response playbook and escalate to higher-ups if necessary.

Q2: How do you validate a true or false positive?

Response: Ask for help. Then review logs, use threat intel sources, and correlate data with other tools.

Q3: What are your immediate next actions upon confirming a breach?

Response: Follow playbook steps-begin containment and notify internal stakeholders.

Q3A: What actions do you take to contain the threat without destroying evidence?

Response: Ask for assistance with firewall rules. Then isolate the server, block malicious IP, and preserve evidence.

Q4: What key information do you gather for leadership and compliance?

Response: Time of breach, data exfiltrated, systems affected, attack vector, destination IP, and containment status.

Q5: What preventative measures would you recommend?

Response: Patch all systems at least twice a year, review logs, and use AI to assist with staff shortages.

Final Recommendations Summary

1. Implement a formal patch management policy (monthly or quarterly).
2. Deploy vulnerability scanners and integrate alerts with ticketing.
3. Enhance log review and enable AI-based threat detection.
4. Invest in endpoint detection, response tools, and network segmentation.
5. Address staffing shortages via MDR or cross-training.
6. Conduct regular tabletop and red team exercises.