HEALTHCARE NETWARS

SANS

Healthcare NetWars is focused on securing the technologies and systems found in the medical field. The challenges task players to solve common cybersecurity tasks such as device vulnerability scanning, web application assessments, and responding to ransomware threats.

Recommended for: Cybersecurity professionals in the healthcare industry, especially those defending electronic medical records, client-facing web applications, and connected medical devices.

"I'm a defender, so knowing how attackers attack is useful. One of the most dangerous attacks in this exercise was flashing firmware on a device that wasn't properly secured. This works in the health and ICS sectors where critical devices aren't secured properly. I work in the health field, so this definitely applies."
- A. W.

Disciplines

- Cyber Defense
- Penetration Testing
- Digital Forensics
- Incident Response
- Log Analysis
- Malware Analysis

Example Topics

- Telemedicine and web app security
- EMR and incident analysis
- Medical device IoT security
- Ransomware analysis and decryption

Computer Requirements

- Internet Access
- Browser-based
  - Chrome
  - Firefox
  - Safari
  - Edge

Interactive Scenario:

Someone has been tampering with Generic Hospital's Electronic Medical Records system. Hired as the lead investigator, you must uncover the attack vectors, prevent further theft, and start the data recovery process. Your task is to uncover artifacts that unmask the culprit for law enforcement. Additionally, you'll need to assess the security of the new web-based application, which is nearly ready for production. Can you rise to the challenge?

Key Specs

CPEs: Up to 6
Delivery: In-person, online, hybrid
Leaderboard: Yes
Levels: Mid, Senior, and Elite
Minimum Seats: 25
Moderator Required: Yes
Player Mode: Solo & Team
Run Time: 6h
Scorecard: Yes

For more information, speak with a SANS Advisor at **sans.org/cyber-ranges/contact**