SentinelCore – Chicago Hospital: Ad Hoc Vulnerability Management Agreement

Company: SentinelCore Security Operations
Client: The Chicago Hospital of Illinois
Prepared by: Jose G.
Date: 12/12/2025

Purpose:
This agreement defines the scope, responsibilities, and process for conducting ad hoc vulnerability scans on client systems upon detection of unusual activity or as requested by the client.

Scope:

- Target system: All Ubuntu servers managed by The Chicago Hospital of Illinois, including inherited or undocumented systems suspected of compromise
- Scan type: Authenticated and unauthenticated vulnerability scans.
- Tools: Tenable or equivalent vulnerability management tools.

Process:

1. Notification: Client informs SentinelCore Security Operations of the need for an ad hoc scan or unusual activity detection.
2. Scope Confirmation: Jose G. confirms target systems, access permissions, and testing boundaries.
3. Baseline Assessment: Assess system for normal behavior before scanning.
4. Connectivity Verification: Confirm system readiness via ping, SSH, and remote access.
5. Vulnerability Scan Execution: Run scans, identify findings, and validate results.
6. Reporting: Provide a detailed report with findings, risk levels, and remediation guidance.

Responsibilities:
SentinelCore Security Operations: Execute scans per agreed scope and SLA; ensure minimal disruption to client operations; maintain confidentiality and integrity of all scanned data.
Client: Provide required credentials and system access; review and act on remediation recommendations.

Confidentiality & Data Handling:
All data collected during ad hoc scans are considered confidential and will not be shared outside SentinelCore Security Operations without client consent.

Acceptance:
By signing below, both parties agree to the terms outlined for ad hoc vulnerability scanning.

Approved by:

Jose G., SentinelCore Security Operations