

Widely recognized Native American healthcare organization strengthens patient privacy by validating cybersecurity controls.

"Breadcrumb helped us validate how our controls performed in practice and gave us greater clarity and confidence in our security posture against real-world threats."

Brandon Herr, IT Director | Southern Indian Health Council (SIHC)

SERVICES DELIVERED

Onsite
Penetration Testing

CIS18-Aligned
Assessment

Public OSINT
Review

Social Engineering
Campaigns

Control
Effectiveness Testing

1 OBJECTIVE

As a healthcare organization, SIHC needed a clear, defensible view of how well its cybersecurity safeguards would perform under realistic conditions. Breadcrumb Cybersecurity was engaged to benchmark SIHC's security posture against CIS18 and determine which controls were operating effectively versus where gaps required focused remediation. The objective was to use assessment and penetration testing results to support risk-based prioritization and practical remediation planning.

2 SOLUTION

Breadcrumb delivered a CIS18-aligned posture assessment paired with practical validation to measure control performance. The engagement integrated control effectiveness testing with an OSINT review and controlled social engineering to evaluate public exposure and human-driven attack paths. Penetration testing validated exploitable conditions and lateral movement opportunities within the environment. Results were mapped to CIS18 objectives and consolidated into a risk-ranked remediation plan.

3 RESULTS

SIHC received decision-ready visibility into which safeguards were reducing risk and where gaps created the most meaningful exposure. The engagement translated technical findings into a prioritized remediation roadmap that SIHC could apply immediately, separating near-term corrective actions from longer-term improvements. This provided a clear basis to focus resources on the changes expected to deliver the greatest risk reduction first.