CLEAR ROI FOR REDSEAL DEPLOYMENT TO SUPPORT VULNERABILITY ASSESSMENT PROGRAM

An anonymous intelligence agency had a problem. Their vulnerability assessment program was expensive and sub-optimal. The program was run by two internal employees and 16 contractors. As they moved from data center to data center, each assessment could take anywhere from 2 months to a full year to conduct.

First the team had to inventory each data center and find all the configuration files. Then they had to review each setup to make sure it was updated and had applied best security practices. Then, they could create a network map.

With the map, the team could, at long last, begin to manually analyze the network for vulnerabilities. Given time and resource constraints, the team was forced to triage. Ignoring medium and low level vulnerabilities, they focused on a short list of the most critical.

Of course, by the time they completed their analysis, the whole network had changed. The network map was merely a snapshot in time. Plus, the vulnerability assessment reports didn't include leapfrogs to move deeper into the network.

The agency realized that getting one or two reports per year on a network that had already changed, at a cost of $5 million, was not a situation that could continue.

After researching various cybersecurity tools and getting a glowing review from other cyber teams in the government, the agency's cybersecurity team discovered RedSeal. RedSeal's continuous monitoring of the config files on the network meant that the network map would never be out of date. In-Q-Tel experts reviewed and quickly approved RedSeal. On a Monday, the team told RedSeal, "We want it on Friday!"

Now, after deploying RedSeal agency-wide and setting up 14 instances, the agency now conducts continuous assessments year round across all data centers. They got rid of the expensive contractors. After five years, their feedback has been 100% positive, "We realize now that we can't leverage the other cybersecurity tools unless we have RedSeal. RedSeal is core to our cybersecurity plan".